# Elektroninen sodankäynti

## osa 1 – taistelun viides dimensio

**Maanpuolustuskorkeakoulu**
**Tekniikan Laitos**

***Julkaisusarja 5***
***No 2/2004***

# Elektroninen sodankäynti

## osa 1 – taistelun viides dimensio

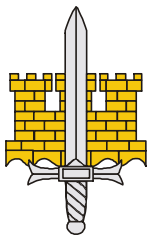
Jyri Kosola, Janne Jokinen

Maanpuolustuskorkeakoulu

Tekniikan laitos

Julkaisusarja 5

No 2



Kannen kuvakollaasi: © J. Kosola 2004
Alkuperäiskuvat:
F-18 Hornet taisteluvarustuksessa [SA-kuva]
Maigret 5000-järjestelmä ja Hummel-ajoneuvo [ewation GmbH/MRCM]

Maanpuolustuskorkeakoulu, Tekniikan laitos
ISBN 951-25-1554-7
ISSN 1795-3294

Edita Prima Oy
Helsinki 2004

# ESIPUHE

Taistelukentän neljä dimensiota, tilavuuteen liittyvät kolme ulottuvuutta ja neljäntenä ulottuvuutena aika, ovat yleisesti tunnettuja ja ihmisten omin aistein havaittavissa. Sen sijaan viides dimensio, sähkömagneettinen spektri, on monille outo ja jo käsitteenäkin epämääräinen. Se muodostuu kuitenkin nykyaikaisessa sodankäynnissä keskeiseksi ulottuvuudeksi ja siinä käytävästä taistelusta tulee välttämättömyys. Sodankäynnissä tiedustelu-, valvonta- ja johtamisjärjestelmien sekä älykkäiden asejärjestelmien rooli on keskeinen. Näiden toimivuus perustuu lähes kokonaan sähkömagneettisen spektrin hyödyntämiseen, minkä vuoksi ne joutuvat alttiiksi vastustajan elektroniselle sodankäynnille.

Elektroniseen sodankäyntiin liittyvä toiminta on ollut ja on edelleen valtioiden tarkimmin varjeltuja salaisuuksia. Tietyn tason jälkeen ovet sulkeutuvat, eikä arvokkaimpia tietoja edelleenkään paljasteta muutoin varsin avoimesta tiedottamisesta huolimatta. Kruununjalokiviä varjellaan viimeiseen asti.

Tämä kirja yrittää selittää ensimmäisen kerran Suomessa, mistä elektronisessa sodankäynnissä on kyse ja minkä vuoksi siihen on välttämätöntä panostaa. Elektronisen sodankäynnin periaatteiden tunteminen auttaa myös ymmärtämään, miksi verkottuminen ja perinteisten sotilaallisen hallinnon rajojen ja hierarkioiden rikkominen on joissain tapauksissa välttämätöntä.

Elektronista sodankäyntiä pidetään sotilaallisissa suurvalloissa yhtenä merkittävimpänä ja kustannustehokkaimpana keinona tehostaa asevoimien suorituskykyä[1]. Esimerkiksi Venäjällä katsotaan, että investoimalla 5-8% perinteisiin asejärjestelmiin käytettävästä summasta elektroniseen sodankäyntiin, tai venäläisittäin *radioelektroniseen taisteluun*, voidaan maavoimien suorituskykyä tehostaa 1,5–2-kertaiseksi, vähentää lentokonetappiot jopa kuudenteen osaan ja laivaston alustappiot kolmanteen osaan siitä, mitä ne olisivat ilman elektronista sodankäyntikykyä. Venäläisen näkemyksen mukaan ELSO:n osuus vastustajan johtamis- ja pääasejärjestelmiin kohdistettavista vaikuttamismenetelmistä nousee 70%:in. Uusien teknologioiden, kuten radiotaajuisten aseiden ja täsmäaseiden käyttö yhdessä ELSO:n kanssa voi lisätä ELSO:n tehokkuutta yli 3-5-kertaisesti[2].

*Elektroninen sodankäynti – taistelun viides dimensio* on tarkoitettu kaikille niille, joiden on ymmärrettävä mitä mahdollisuuksia ja uhkia elektroninen sodankäynti luo sodankäyntiin ja sotilaallisten operaatioiden suorittamiseen sekä miten ELSO tulisi integroida osaksi muuta sodankäyntiä.

Kirjassa on pyritty korostamaan operatiivis-taktisen tason näkökulmaa. Kirjan tavoitteena on se, että lukija ymmärtää

- miten elektroninen sodankäynti kykenee tukemaan omaa sotilaallista operaatiota

- miten elektronisella sodankäynnillä voidaan ratkaisevissa tilanteissa haitata, estää tai hidastaa vastustajan toimintaa
- miten vastustaja kykenee paljastamaan oman operaatiomme ja miten se pyrkii vaikuttamaan operaatiomme toteuttamiseen
- miten vastustajan toimien vaikutus tulee ottaa huomioon omassa operaatiossamme

Kirjassa on pyritty kuvaamaan elektronisen sodankäynnin roolia ja menetelmiä operaatioiden toteuttamisen, sotilaallisen suorituskyvyn ja toimintavalmiuden kannalta optimaalisessa tilanteessa. Nykytilanne Suomessa sen paremmin kuin ulkomaillakaan ei välttämättä kaikilta osin vastaa tätä tavoitetilaa.

Aihepiirin yleisestä sensitiivisyydestä huolimatta kirja ei ole tietoturvaluokiteltu. Kirjan julkisuus rajaa luonnollisesti joitakin aihepiirejä ja tarkastelutasoja pois ja pakottaa useissa kohdin ottamaan teoriaa valaisevia esimerkkejä nykypäivän sijasta sotahistoriasta. Kirjassa käsitellään kuitenkin huomattavan laajasti ja yksityiskohtaisesti aihepiiriä, josta Suomessa ei tähän asti ole totuttu puhumaan julkisuudessa.

Kirja ei käsittele elektronisen sodankäynnin tekniikkaa eikä menetelmiä. Näihin liittyviä asioita on kuitenkin esitetty kirjan lukuisissa liitteissä, joihin on sisällytetty sinisellä painettuja havainnollistavia esimerkkejä. Tiedustelu-, valvonta-, johtamis- ja asejärjestelmien elektronisen suojaamiseen sekä elektronisen sodankäynnin tekniikkaan ja menetelmiin voi perehtyä esim. Maanpuolustuskorkeakoulun kirjan *Digitaalinen taistelukenttä – informaatioajan sotakoneen tekniikka*[3] avulla.

Haluamme lausua erityiset kiitokset tekstin tarkastukseen osallistuneille sekä kuvamateriaalia ja arvokkaita neuvojaan tarjonneille henkilöille, joista mainittakoon eversti Jari Kähärä, insinöörieverstiluutnantti Tapio Halkola, insinöörieverstiluutnantti Seppo Heiskanen, insinöörimajuri Olli Klemola, majuri Harri Roivainen, majuri Pasi Jokinen, insinööriyliluutnantti Tero Solante ja TkL Timo Pulkkinen.

Helsingissä 15.11.2004

tekijät

---

Insinöörimajuri **Jyri Kosola** on suorittanut diplomi-insinöörin ja tekniikan lisensiaatin tutkinnot Teknillisessä Korkeakoulussa sekä M.Sc.-tutkinnon elektronisessa sodankäynnissä Royal Military College of Sciencessä Englannissa ja opiskelee tällä hetkellä yleisesikuntaupseerikurssi 52:lla Maanpuolustuskorkeakoulussa. Kosola on palvellut Puolustusvoimissa vuodesta 1991 alkaen erilaisissa sotilaselektroniikkaan, johtamisjärjestelmiin ja ELSO:on sekä informaatiosodankäyntiin liittyvissä tehtävissä.

Insinöörikapteeni **Janne Jokinen** on suorittanut filosofian maisterin ja tohtorin tutkinnot Helsingin yliopistossa sekä Master of Science -tutkinnon sotilaselektroniikkajärjestelmissä ja elektronisessa sodankäynnissä Royal Military College of Sciencessä Englannissa. Jokinen on palvellut Puolustusvoimissa vuodesta 1997 alkaen elektroniseen sodankäyntiin liittyvissä tehtävissä.

# SISÄLLYS

ESIPUHE ..... 3

SISÄLLYS ..... 5

1. ELEKTRONISEN SODANKÄYNNIN MERKITYS JA ROOLI TAISTELUSSA ..... 9
*Laadun voitto määrästä ..... 9*
*Sähkömagneettisen spektrin hallinta on kriittinen taistelutekijä ..... 10*
*Sähkömagneettinen toimintaympäristö ..... 13*
*Elektroninen taistelukenttä ..... 17*
*Elektronisen sodankäynnin rooli sotilasoperaatioissa ..... 19*
*ELSO informaatiosodankäynnin työkaluna ..... 20*
Informaatiosodankäynnin käsite ..... 20
Informaatio-operaatiot ..... 23
Vaikutuspohjainen maalitus ..... 24
ELSO fyysisen vaikuttamisen tukena ..... 26
ELSO operaatioturvallisuuden tukena ..... 27
ELSO operatiivisen harhauttamisen tukena ..... 28
ELSO psykologisen operaation tukena ..... 29
ELSO tietojärjestelmäsodankäynnin tukena ..... 29

2. ELEKTRONISEN SODANKÄYNNIN ELEMENTIT ..... 30
*Elektroninen tuki ..... 31*
Operatiivinen elektroninen tiedustelu ja valvonta ..... 33
Elektroninen maalinosoitus ..... 37
Elektroninen uhkavaroitus ..... 39
*Elektroninen vaikuttaminen ..... 39*
Elektroninen häirintä ..... 40
Elektroninen harhauttaminen ..... 43
Elektroninen lamauttaminen ja tuhoaminen ..... 44
*Elektroninen suojautuminen ..... 47*
Suojautuminen elektroniselta tiedustelulta ja sen tukemalta asevaikutukselta ..... 47
Suojautuminen elektroniselta vaikuttamiselta ..... 48
Suojautuminen asejärjestelmiltä ..... 49
Sotamoodien käyttö elektronisen suojautumisen turvaamisessa ..... 52
*Elektronisen sodankäynnin tukitoiminta ..... 54*
*Puolustushaarakohtaisia vivahteita ..... 56*

3. ELEKTRONISEN SODANKÄYNNIN LIITYNNÄT MUIHIN TOIMINNAN ALOIHIN ..... 66
*Tiedustelu ..... 66*
*Signaalitiedustelu ..... 67*
*Taajuushallinta ..... 69*
Taajuushallinnan rooli sotilaallisissa operaatioissa ..... 69
Taajuushallinnan toteutus puolustusvoimissa rauhan aikana ..... 71
*Häivetekniikka ja elektroninen sodankäynti ..... 74*
*Harhautus elektronisen sodankäynnin tukena ..... 75*
Harhautus elektronisen tiedustelun ja valvonnan tukena ..... 76
Harhautus elektronisen vaikuttamisen tukena ..... 77
Harhautus elektronisen suojautumisen tukena ..... 77
*Fyysinen vaikuttaminen elektronisen sodankäynnin tukena ..... 78*
*Psykologinen sodankäynti elektronisen sodankäynnin tukena ..... 79*

4. ARVIO ELSO:N ELEMENTTIEN KEHITTYMISESTÄ TULEVAISUUDESSA ..... 81
*Elektroninen tuki* ..... *81*
*Elektroninen vaikuttaminen* ..... *85*
*Elektroninen suojautuminen* ..... *88*
*ELSO-tukitoiminta* ..... *93*

5. TIETOTURVALLISUUS ELEKTRONISESSA SODANKÄYNNISSÄ ..... 94
*Salassapito on suorituskyvyn edellytys* ..... *94*
*Salailu heikentää saavutettavissa olevaa suorituskykyä* ..... *96*
*Tietoturvaluokituksen lähtökohdat* ..... *98*

6. ELEKTRONISEN SODANKÄYNNIN HUOMIOIMINEN KEHITTÄMISOHJELMISSA ..... 99

7. ELEKTRONINEN SODANKÄYNTI SOTAHISTORIASSA ..... 102
*Elektronisen tuen antamat tiedot ovat oikein käytettyinä avain voittoon* ..... *102*
*Suhteellinen etu vastustajaan nähden voi olla olemassa vain lyhyen ajan* ..... *103*
*Olennaista on tuntea vastapuolen järjestelmät* ..... *104*
*Myös omien järjestelmien tunteminen on tärkeätä* ..... *104*
*Salassapito on usein edellytys toiminnan onnistumiselle* ..... *105*
*Liika salassapito saattaa estää toiminnan onnistumisen* ..... *105*
*Harhautus tukee tehokkaasti elektronista suojautumista* ..... *106*
*ELSO on tehokkain joukon suorituskykyä lisäävä tekijä* ..... *106*
*ELSO:n käyttöperiaatteita ja kokemuksia Venäjän sodissa tshetsheenejä vastaan* . *109*
Ensimmäinen sota 1994-1996 ..... 110
Toinen sota 1999 alkaen ..... 115
Venäläisten kehittämiskohteet ensimmäisen sodan jälkeen ja niiden huomiointi toisen sodan aikana ..... 116
*Johtopäätöksiä historiasta* ..... *120*

8. YHDISTELMÄ JA JOHTOPÄÄTÖKSET ..... 121

## LIITTEET

LIITE 1: SÄHKÖMAGNEETTINEN SPEKTRI ..... 125
*Radiotaajuinen säteily* ..... *125*
*Optinen säteily* ..... *127*

LIITE 2: SUOJAUTUMINEN ELEKTRONISELTA TIEDUSTELULTA JA VALVONNALTA ..... 129
*Edellytykset elektroniselle tiedustelulle paljastumiselle* ..... *129*
*Suojautuminen elektroniselta tiedustelulta* ..... *131*
*Paljastumisetäisyyden määrittäminen* ..... *132*
*Paikantamistarkkuuden arviointi* ..... *142*

LIITE 3: SUOJAUTUMINEN ELEKTRONISELTA HÄIRINNÄLTÄ ..... 146
*Edellytykset järjestelmän häiriintymiselle* ..... *146*
*Yleisiä toiminnallisia keinoja suojautua häirinnältä* ..... *147*
*Viestijärjestelmien suojaaminen* ..... *150*
*Tutkajärjestelmien suojaaminen* ..... *162*

LIITE 4: RADIOTAAJUISET ASEET ..... 166

LIITE 5: ELEKTRONISEN SODANKÄYNNIN TEKNIIKKAAN LIITTYVIÄ KÄSITTEITÄ ..... 170
*Desibeli – joustava tapa käsitellä tehoyksiköitä ..... 170*
*Taajuus ja aallonpituus ..... 172*
*Antenni – keskeinen järjestelmän suorituskykyyn vaikuttava tekijä ..... 172*
*Vastaanotin – tasapainoilua eri vaatimusten ja luonnonlakien välillä ..... 175*
*Signaalien tehobudjetti – yksisuuntaisen yhteyden neliölaki ..... 176*
*Signaalien tehobudjetti – tutkan neljännen potenssin laki ..... 178*
*Häirinnän ja hyötysignaalin taistelu ..... 179*
*Infrapunasäteilyn ominaisuuksia – jokainen säteilee, haluaa tai ei ..... 183*

LIITE 6: HARJOITUSVASTUSTAJAN ELSO-JOUKOT ..... 187
*Johdanto ..... 187*
*Elektroninen sodankäynti vastustajan informaatio-operaatioissa ..... 188*
*Elektronisen sodankäynnin toteuttaminen ..... 190*
*ELSO:n elementtien käyttö taistelussa ..... 191*
Elektroninen tuki ..... 191
Elektroninen vaikuttaminen ..... 192
Elektroninen suojautuminen ..... 194
*ELSO-joukot OPFOR:n organisaatioissa ..... 195*
Prikaatin orgaaniset ELSO-joukot ..... 195
Divisioonan orgaaniset ELSO-joukot ..... 195
Armeijakunnan ja armeijan ELSO-joukot ..... 196
Armeijaryhmän ELSO-joukot ..... 198
Muut ELSO-joukot ..... 200

LIITE 7: KÄSITTEET JA MÄÄRITELMÄT ..... 201

LIITE 8: KÄYTETYT LYHENTEET ..... 210

LIITE 9: LÄHDEVIITTEET JA HUOMAUTUKSET ..... 216

# 1. ELEKTRONISEN SODANKÄYNNIN MERKITYS JA ROOLI TAISTELUSSA

## Laadun voitto määrästä

Länsimaissa vallalla olevan ajattelumallin mukaan taistelun voittoon pyritään iskemällä vastustajan kriittisiin kohteisiin strategisella, operatiivisella ja taktisella tasolla koko sen syvyydessä. Taistelussa on kyettävä ylläpitämään liikettä, löydettävä vastustajan toiminnan kannalta kriittiset kohteet sekä iskettävä niihin nopeasti, yllättävästi ja keskitetyllä voimalla. Voitto saavutetaan hidastamalla vastustajan toimintaa samalla kun itse ylläpidetään omaa operatiivista ja taktista taistelutempoa. Tämä edellyttää muun muassa:

- kykyä valvoa reaaliaikaisesti taistelutilaa ja sähkömagneettista spektriä syvältä vastustajan hallussa olevalta alueelta kauas omaan selustaan
- kykyä löytää ja paikantaa todelliset maalit sekä erottaa ne vastustajan harhautuksesta tai taistelun kannalta merkityksettömistä kohteista
- kykyä välittää tulenkäyttöön liittyvää informaatiota kaukana vastustajan syvyydessä toimivilta sensoreilta kaukana omassa selustassa sijaitseville asejärjestelmille
- kykyä suunnata asevaikutusta havaittuihin maaleihin muutamissa sekunneissa tai minuuteissa havainnosta
- kykyä varmistaa ohjusten ja muiden hakeutuvien tai ohjattavien aseiden osuminen maaleihinsa sekä havaita aseilla aikaan saatu vaikutus
- kykyä kerätä taistelukentällä hajallaan olevilta joukoilta tietoja ja johtaa niitä niiden ollessa liikkeessä

Vastaavasti vastustajan hidastaminen edellyttää vaikuttamista yhteen tai useampaan vastustajan kokonaistoiminnan kannalta kriittisistä elementeistä: sensori- tiedonsiirto-, päätöksenteko- tai asejärjestelmään.

Tehokkain keino oman taistelutemmon ja taktisen toimintavapauden ylläpidossa on varmistaa johtajille ja asejärjestelmille riittävän reaaliaikainen tietoisuus ympäröivästä tilanteesta. Paremman – siis reaaliaikaisemman ja tarkemman – *tilannetietoisuuden* (SA, Situational Awareness) omaava saavuttaa informaatioylivoiman vastustajastaan. ***Informaatioylivoima*** (IS, Information Superiority) on suhteellinen ylivoima informaatio-operaatiossa vastustajaan nähden ajantasaisen informaation keräämisessä, käsittelemisessä ja jakamisessa. Informaatioylivoima saavutetaan sekä tukemalla omaa informaatioprosessia että heikentämällä vastustajan informaatioprosessia. Venäläisen käsityksen mukaan ***informaatioylivoiman hankkiminen mahdollistaa omien joukkojen ryhmittämisen sekä elektronisen sodankäynnin, tulivaikutuksen ja erikoisjoukkojen käytön siten, että operaation tavoitteet on saavutettu jo ennen***

***varsinaisten sotatoimien puhkeamista***[4]. Ajatus sodan voittamisesta jo ennen taisteluiden aloittamista on yhdenmukainen myös länsimaisen käsityksen kanssa. Vaikka vastustaja ei tunnustaisikaan häviötään jo ”informaatioiskuvaiheessa”, on sen tappio sotatoimissa kuitenkin jo sinetöity, mikäli toinen osapuoli kykenee saavuttamaan riittävän informaatioherruuden.

Voittoon pyritään nykyään siis nimenomaan informaatioylivoiman avulla. Informaatioylivoima taistelutilassa saavutetaan älykkäillä ja *toisiinsa verkotetuilla* sensoreilla, johtamisjärjestelmillä sekä asejärjestelmillä[a]. Tällaisesta älykkäästä verkotetusta kokonaisuudesta käytetään erilaisia nimityksiä eri maissa, kuten verkostokeskeinen sodankäynti (NCW, Network-Centric Warfare, USA), verkon mahdollistama suorituskyky (Network-Enabled Capability, UK) tai verkkokeskeinen puolustus (NBF, Net-Baserad Försvar, Ruotsi). Sensoreiden, asejärjestelmien ja johtajien verkottamisen etuna on kyky valvoa laajaa taistelutilaa ja kohdentaa vastustajaan tulta riippumatta siitä, missä omat joukot ja järjestelmät ovat, sekä kyky keskittää nopeasti tulivaikutus yllättäviinkin suuntiin. Kokonaisjärjestelmä on kuitenkin hyvin riippuvainen tiedustelutietojen saamisesta, oikeasta tilannekuvasta, johtoportaiden ja yksiköiden sekä sensoreiden ja asejärjestelmien välisestä tiedonsiirrosta[5]. Tämä puolestaan johtaa lähes täydelliseen riippuvuuteen sähkömagneettisesta spektristä ja sähköisestä tiedonsiirrosta.

## Sähkömagneettisen spektrin hallinta on kriittinen taistelutekijä

***Spektrin kokonaishallinnasta on tullut yksi taistelun kriittisistä tekijöistä.***

Sähkömagneettista säteilyä[6] hyödynnetään sodankäynnissä tiedon siirtämiseen tiedustelu-, valvonta-, johtamis- ja asejärjestelmien osien välillä, toimintaympäristön havaitsemiseen erilaisin sensorein, joukkojen ja järjestelmien paikantamiseen ja navigointiin, omien ja vihollisten erottamiseen toisistaan, älykkäiden aseiden ohjaamiseen maaliinsa sekä oikean ja tarkan ajan välittämiseen erilaisiin korkeateknologisiin järjestelmiin. Vaikuttaminen vastustajan syvyyteen sen hyvin suojattuihin kriittisiin pisteisiin edellyttää kykyä lamauttaa ainakin tilapäisesti vastustajan valvonta-, johtamis- ja suojausjärjestelmät. Vastaavasti puolustautuminen vastustajan hyökkäyksiltä edellyttää omien tiedustelu-, valvonta-, johtamis-, omasuoja-, omatunnistus- ja asejärjestelmien suojaamista. Koska sekä puolustajan, että hyökkääjän toiminta perustuu kokonaan sähkömagneettisen spektrin hyväksikäyttöön, spektrin kokonaishallinnasta on tullut yksi taistelun kriittisistä tekijöistä[7].

***Spektrin hallinnan defensiiviset elementit*** ovat taajuushallinta, emissiokontrolli ja järjestelmien elektroninen suojaaminen. ***Taajuushallinnalla*** tarkoitetaan taajuuksien

[a] Verkotetusta sensori- ja maalinosoitusjärjestelmästä käytetään myös nimitystä ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance eli tiedustelu, valvonta ja maalinosoitus)

jakamista järjestelmien käyttöön sekä joukkojen spektrin käytön ohjausta ja valvontaa. ***Emissiokontrollilla*** tarkoitetaan sitä, että yhtymän spektrin käyttö suunnitellaan, valvotaan ja ohjataan osana yhtymän operatiivista toimintaa[b]. Emissiokontrollin suunnittelun perusteet tulevat lähinnä operaatioturvallisuuden vaatimuksista, jotka puolestaan saadaan komentajan tekemästä toiminnan perusajatuksesta.

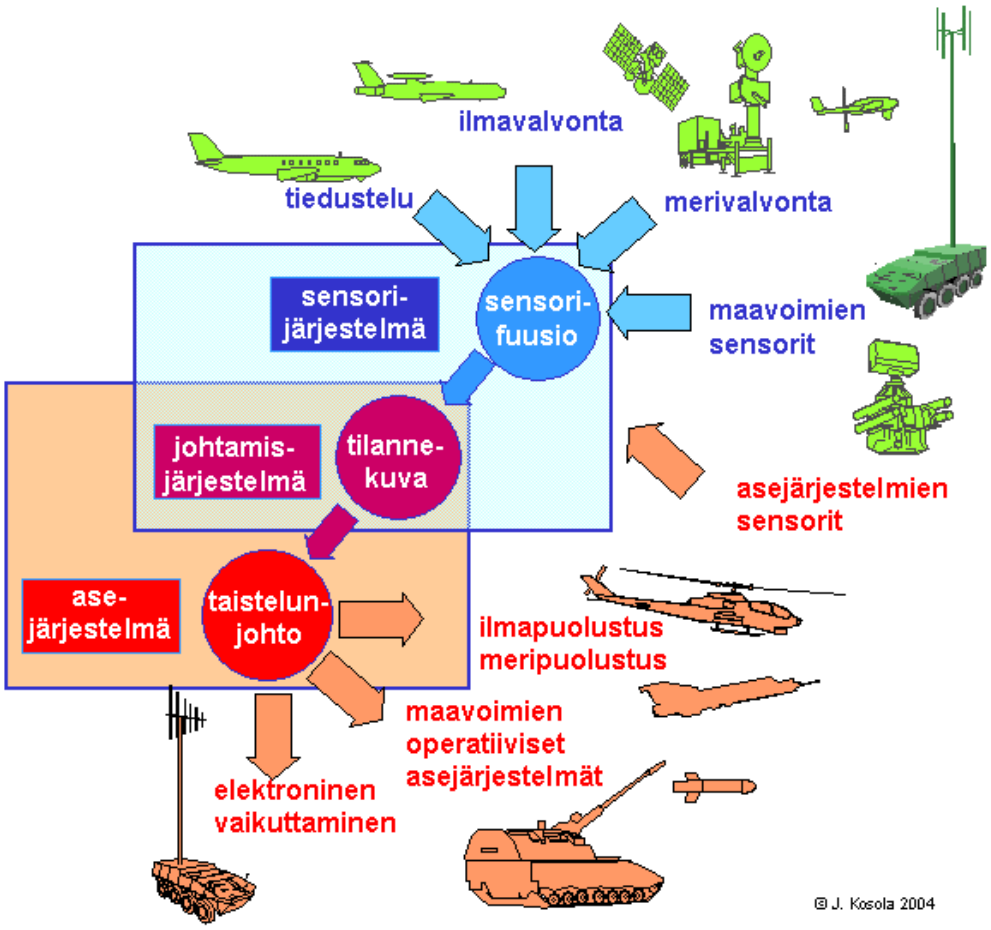

**Kuva 1: Liikesodankäynti edellyttää reaaliaikaista tilannekuvaa ja hajallaan toimivien joukkojen johtamiskykyä. Siten johtamisjärjestelmän elektroninen suojaaminen on välttämätön edellytys taistelukyvylle.** [J. Kosola]

Oman spektrin käytön hallintaan liittyen on varmistettava, etteivät omat lähettävät ja vastaanottavat järjestelmät häiritse toisiaan. Ohjattavia laitteita on suuri määrä tietoliikennejärjestelmistä aktiivisiin sensoreihin, kuten tutka ja lasertutka, ja passiivisiin sensoreihin, kuten kuvaavat passiiviset millimetriaaltojärjestelmät. Radiotaajuisten aseiden sekä perinteisen elektronisen sodankäynnin vaikuttamiskeinojen käyttö asettaa ongelmia erityisesti taajuuskaistan käytettävyydelle: joillakin spektrin alueilla elektroninen vaikuttaminen voi haitata tai jopa estää omien järjestelmien käytön.

Vastustajan spektrin käyttöä ei voida täysin estää. Se voi kuitenkin olla mahdollista halutulla hetkellä valitussa paikassa ja halutuilla taajuuksilla. ***Spektrin hallinnan offensiiviset elementit*** sisältävät elektroniseen sodankäyntiin kuuluvan elektronisen häirinnän ja lamauttamisen lisäksi fyysisen tulenkäytön vastustajan elektronisia järjestelmiä vastaan.

[b] NATO:n käsitemaailmassa emissiokontrolli EMCON (Emission Control) on osa operatiivisen alan vastuulla olevaa elektronista sodankäyntiä, kun taas taajuushallinta on osa johtamisjärjestelmäalaa.

Nykyaikaisella taistelukentällä taajuushallinta on suuri haaste ilman vastustajan käyttämien taajuuksien aiheuttamia häiriöitä ja tahallista häirintääkin. Tekninen kehitys on johtanut siihen, että vastustajaa häirittäessä vaikeutetaan samalla helposti myös omien joukkojen toimintaa. Näin elektronisella vaikuttamisella voidaan heikentää omaa elektronista suojautumista. Elektronisen vaikuttamisen hyödyntäminen on siten hyvin samanlaista kuin muidenkin asejärjestelmien käyttö ja vaatii paitsi kaikkien käytettävissä olevien välineiden käytön keskinäistä koordinointia, myös reaaliaikaista tilannekuvaa.




**Kuva 2: Tulevaisuuden integroitu yhteinen (*joint*-) puolustusjärjestelmä koostuu toisiinsa verkotetuista sensoreista, joiden tiedot yhdistetään yhtenäiseksi tilannekuvaksi sekä yhtenäisestä johtamisjärjestelmästä ja sen ohjaamasta verkotetusta asejärjestelmästä.**

Sodankäynnissä vallitsee jatkuva kilpailu menetelmän ja vastamenetelmän välillä. Selkeimmin miellettävä kilpailuasetelma on panssarin suojan ja panssarin läpäisyn välinen kilpa-asetelma, jossa koko ajan pyritään kehittämään vaikeammin läpäistävää panssarointia ja toisaalta läpäisykykyisempiä aseita. Sama kilpa-asetelma vallitsee

sähkömagneettisessa spektrissä: kun toinen osapuoli kehittää järjestelmän, joka hyödyntää sähkömagneettista spektriä johonkin toimintaansa (measure), toinen osapuoli pyrkii yleensä kehittämään toisaalta järjestelmän, jolla tiedustelee ja valvoo vastustajan spektrin käyttöä ja toisaalta järjestelmän, jonka avulla estää vastustajaa käyttämästä spektriä haluamaansa käyttötarkoitukseen (counter-measure). Vastaavasti vastustaja pyrkii kehittämään vastatoimenpiteitä, joilla toisen osapuolen vasta-toimenpiteet väistetään tai vältetään (counter-counter-measure) ja edelleen suojautuja pyrkii kehittämään keinon, jolla mitätöidään vastustajan vastakeino omalle suojautumiselle (counter-counter-counter-measure)[c]. Ketjua voisi jatkaa loputtomiin. Olennaista on tunnistaa, että spektrin käyttöön liittyy aina

- sähkömagneettisen säteilyn hyödyntäminen johonkin tarkoitukseen, yleensä joko tiedon siirtoon tai keräämiseen taistelukentältä.
- vastustajan spektrin käytön valvonta, jolla saadaan kerättyä vastustajan toiminnasta tietoja
- vastustajan spektrin käytön estäminen tai vaikeuttaminen, jolla saadaan estettyä tai vaikeutettua vastustajan sotilaallista toimintaa
- oman sähkömagneettisen spektrin käytön turvaaminen vastustajan toiminnalta

Elektronisen sodankäynnin termeinä sähkömagneettisen spektrin valvonnasta käytetään nimitystä elektroninen tuki (ELTU, engl. Electronic Support, ES), spektrin käytön estämisestä ja vaikuttamisesta nimitystä elektroninen vaikuttaminen (ELVA, engl. Electronic Attack, EA)[8]. Vastustajan elektroniselta tuelta ja vaikuttamiselta suojautumisesta käytetään nimitystä elektroninen suojautuminen (ELPU, engl. Electronic Protection, EP).

## Sähkömagneettinen toimintaympäristö

Sähkömagneettinen säteily on vaihtelevan sähkö- ja magneettikentän aaltoliikettä, joka etenee tyhjössä ja ilmassa valon nopeudella ja esimerkiksi metallijohtimissa hyvin lähellä (eli noin 60-70%) sitä. Hyvä muistisääntö valon nopeudelle on se, että säteily etenee 300 metriä mikrosekunnissa eli sekunnin miljoonasosassa. Säteily ei tarvitse edetäkseen mitään väliainetta, sillä ilmiö perustuu siihen, että vaihteleva sähkökenttä synnyttää vaihtelevan magneettikentän, joka puolestaan synnyttää sähkökentän jne.

[c] Aiemmin elektronisista vastatoimista, kuten häirinnästä, käytettiin nimitystä ECM (Electronic Counter-Measures) ja vastatoimien (häirinnän) vastatoimista (siis suojautumisesta vastustajan vastatoimia vastaan) nimitystä ECCM (Electronic Counter-Counter-Measures). Koska vastatoimien ketju jatkuu periaatteessa loputtomiin, on pitkät nimitykset korvattu yksinkertaisesti elektronisella vaikuttamisella (vastustajan järjestelmiin) ja elektronisella suojautumisella (vastustajan elektroniselta vaikuttamiselta).

Sähkömagneettista säteilyä voidaan synnyttää esimerkiksi radio- tai tutkalähettimessä, josta se antennin avulla lähetetään tiettyyn suuntaan. Vastaanotin puolestaan kykenee antenninsa avulla havaitsemaan tietystä suunnasta tulevan sähkömagneettisen säteilyn, ja siihen lähettimessä mahdollisesti koodatun (*moduloidun*) informaation. Sähkömagneettinen säteily etenee periaatteessa suoraviivaisesti, joskin tietyissä tilanteissa se voi esimerkiksi taipua, heijastua tai sirota eri suuntaan. Sähkömagneettista säteilyä voi myös syntyä ihmisen aktiivisista toimista riippumatta, esimerkiksi kaikkien kappaleiden lähettämänä lämpösäteilynä.

Säteilyä kuvaavista suureista keskeisin on taajuus, joka kertoo kuinka monta kertaa sekunnissa sähkö- tai magneettikenttä värähtelee. Taajuuden yksikkö on hertsi [Hz] ja sen yleisimmin taistelukentällä esiintyvät kerrannaiset ovat kilohertsi kHz (tuhatta hertsiä), megahertsi MHz (tuhatta kHz eli miljoonaa hertsiä) ja gigahertsi GHz (tuhatta MHz eli miljardia hertsiä)[9].

Käsite sähkömagneettinen spektri kuvaa sitä taajuusaluetta, jolla sähkömagneettista säteilyä esiintyy. Liitteessä 1 on kuvattu sähkömagneettisen spektrin jakautuminen osiin ja näille osille annetut nimet. Sotilaallisessa mielessä kiinnostava sähkömagneettinen spektri voidaan jakaa karkeasti ottaen kahteen alueeseen:

- radiotaajuiseen osaan ja
- optiseen osaan.

Radiotaajuinen osa voidaan niin haluttaessa jakaa radio- ja tutka-alueisiin, vaikka jako onkin teennäinen. Radiotaajuisen spektrin osan mittayksikkönä käytetään yleisimmin taajuutta. Optinen spektri jaetaan infrapuna-alueeseen, näkyvän valon alueeseen ja ultraviolettialueeseen. Optisella alueella käytetään mittayksikkönä aallonpituutta, joka on visuaalisella ja ultraviolettialueella nanometrien (nm) luokkaa ja infrapuna-alueella mikrometrien (µm) luokkaa.

Toimintaympäristössä esiintyy aina sekä luonnossa normaalisti esiintyvää sähkömagneettista säteilyä että ihmisen aikaansaamaa säteilyä. Näitä molempia hyödynnetään sodankäynnissä. Toisaalta sekä ihmisen synnyttämästä että luonnosta peräisin olevasta säteilystä on myös haittaa sotilaallisten järjestelmien toiminnalle. Sähkömagneettisen ympäristön vaikutusta sotilaallisiin järjestelmiin kutsutaan termillä E3 (Electromagnetic Environmental Effects). E3 käsittää:

1. laitteiden ja järjestelmien sähkömagneettisen yhteensopivuuden[10]
2. järjestelmien elektronisen suojautumisen ulkoisilta uhkilta
3. sähkömagneettisen säteilyn ja staattisen sähkön purkausten synnyttämän vaikutuksen räjähteisiin[11], polttonesteisiin ja elektronisiin laitteisiin[12]

Sähkömagneettisessa spektrissä esiintyvällä säteilyllä voi olla useita haitallisia vaikutuksia sotilaallisten järjestelmien toimintaan:

1. ***Kohina*** on fysikaalinen ilmiö, jota esiintyy kaikissa sähköisissä laitteissa. Se voi olla esim. elektronien lämpöliikkeestä aiheutuvaa ***lämpökohinaa***, puolijohdelaitteissa esiintyvää ***raekohinaa*** tai vaikkapa antennin kautta järjestelmään tulevaa ***kosmista kohinaa***. Kohina heikentää järjestelmien suorituskykyä pienentämällä suurinta mahdollista kantamaa, yhteys-etäisyyttä, informaation siirtonopeutta tms. suorituskykyparametria. Osa kohinasta syntyy laitteiden sisällä tai vaikkapa kaapeloinneissa. Osa kohinasta on peräisin ulkomaailmasta, osa jopa ulkoavaruudesta. Tällaista pienitehoista taustakohinaa esiintyy siten kaikkialla. Kohinaa syntyy myös viallisissa tai huonosti suunnitelluissa elektronisissa laitteissa, autojen ja voimakoneiden moottoreiden sytytysjärjestelmissä yms. ihmisen luomissa sähköisissä järjestelmissä. Järjestelmien suorituskykyyn kohina saattaa vaikuttaa erityisesti ryhmitettäessä joukkoja esimerkiksi teollisuusalueille tai taajamiin.

2. Mikäli kohina on järjestelmän omaan signaalitasoon nähden riittävän suuritehoista, se voi saada aikaan virheen informaation vastaanotossa, esimerkiksi tiedonsiirtolaite tulkitsee siirretyn symbolin väärin, sensori antaa väärän hälytyksen jne. Kohinatasoa voidaan nostaa myös ***elektronisella häirinnällä***, jolloin esimerkiksi tiedonsiirto- ja tutka-vastaanottimet alkavat toimia virheellisesti.

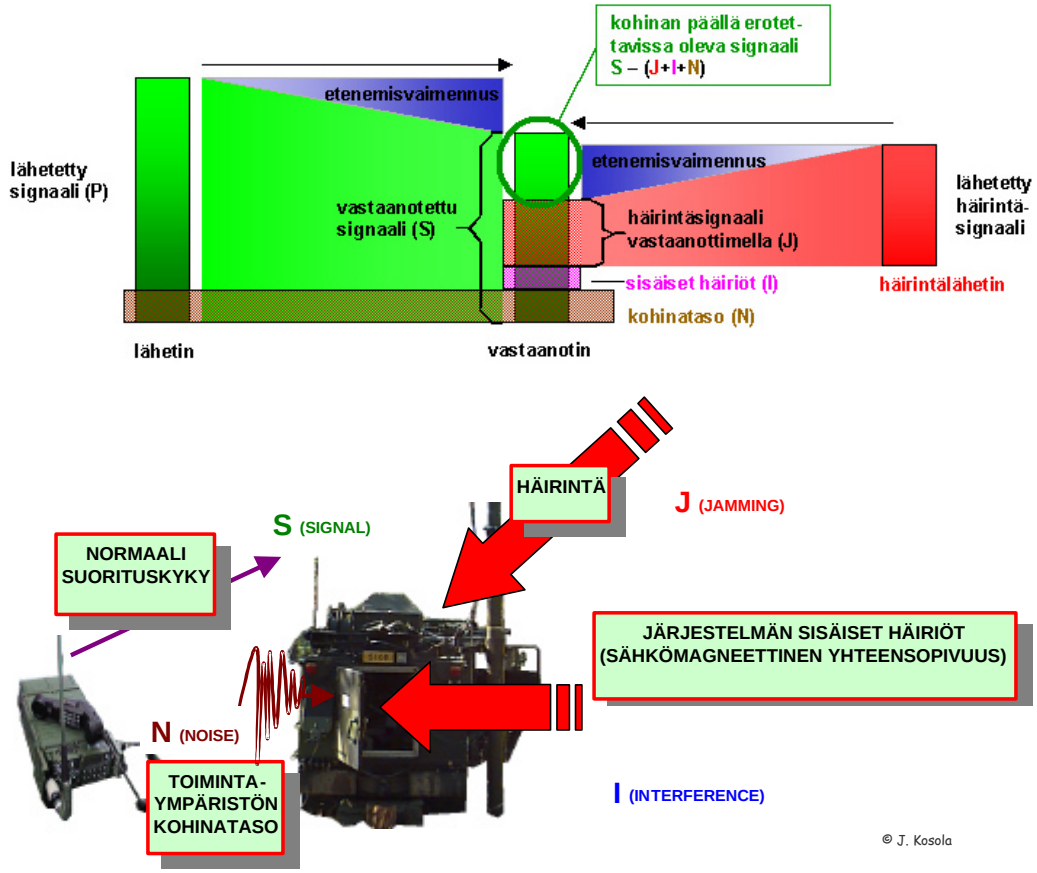
3. Mikäli kohina on hyvin voimakasta, se voi synnyttää ns. ***transienttipulssin***, joka saa aikaan häiriön elektronisen laitteen toiminnassa, esimerkiksi kaataa tietokoneen.

4. Erittäin korkeatehoinen häiriö voi aiheuttaa pysyvän vaurion elektroniseen laitteeseen. Pysyvään vaurioon riittävä teho voi olla peräisin esimerkiksi salamasta tai jonkinlaisesta sähkömagneettista säteilyä lähettävästä aseesta.

Sähkömagneettisen säteilyn hyödyntäminen perustuu siihen, että sen kautta otetaan vastaan energiaa, jonka perusteella tehdään johtopäätöksiä, esimerkiksi onko tutkakaikuna tulleessa lähetteessä havaittavissa lentokoneesta aiheutunut heijastus. Kun säteily etenee lähettimeltä vastaanottimelle, se vaimenee useista syistä. Säteilyn leviäminen laajemmalle alueelle vaimentaa sen tehotiheyttä etäisyyden kasvaessa. Mitä tarkemmin säteily saadaan kohdistettua vastaanottimeen, sitä vähemmän se vaimenee, mutta väistämättä vaimennusta tapahtuu etäisyyden mukana. Tämän *vapaan tilan vaimennuksen* (free-space loss) lisäksi säteily vaimenee etenemisreitillä olevien esteiden tai vaimentavan materiaalin vuoksi. Ennen pitkää jollakin etäisyydellä lähettimestä tullaan tilanteeseen, jossa *signaali* (säteilyn teho) on vaimentunut kohinan tasolle. Mikäli vastaanottimessa ei olisi lainkaan kohinaa, voitaisiin signaali ottaa vastaan ja tulkita oikein äärettömän pitkältä etäisyydeltä. Käytännössä kohinataso määrää kuinka pienitehoinen signaali vielä voidaan tulkita oikein.

Kuvassa 3 on esitetty, miten lähetetty signaali $T$ vaimenee etenemisvaimennuksen $L$ vuoksi vastaanottimessa vastaanotetuksi signaaliksi $S = T - L$. Vastaavasti

häirintälähettimestä tuleva signaali vaimenee tasoon *J* edetessään häirintälähettimeltä häirinnän kohteena olevalle vastaanottimelle. Vastaanottimen oma kohinataso on *N* ja järjestelmän sisäiset häiriöt ovat tasolla *I*. Tällöin vastaanotetun signaalin *S* tulkintaa haittaava säteily on tasolla *J* + *I* + *N*. Tämän summautuneen kohinan päällä erotettavissa olevan signaalin suuruudesta riippuu, toimiiko järjestelmä. Vaadittava S – (J+I+N) –suhde vaihtelee järjestelmittäin: joissakin järjestelmissä toimintakyky romahtaa, vaikka häirintäsignaalin teho olisi vain kymmeniä prosentteja hyötysignaalin tehosta, kun taas joidenkin erityisen hyvin suojattujen järjestelmien häiritseminen vaatii tuhansia kertoja hyötysignaalia suurempaa häirintätehoa. Järjestelmien häirittävyyttä tarkastellaan lähemmin liitteessä 3.




**Kuva 3: Järjestelmän suorituskykyä – esimerkiksi viestijärjestelmän kantamaa – heikentää vastustajan häirinnän (*J*) lisäksi järjestelmän sisäinen häiriötaso (*I*) ja asemapaikan toimintaympäristön ja vastaanottimen kohinataso (*N*). Suorituskyvyn määrittää kohinan päällä erotettavissa olevan signaalin taso: *S* – (*J*+*I*+*N*).**

On syytä huomata, että sähkömagneettisen ympäristön aikaansaamat toimintahäiriöt, sen asettamat rajoitukset tai aiheuttamat vauriot eivät sinänsä riipu siitä, mikä on toimintahäiriötä tai vaurioita aiheuttavan säteilyn lähde. Esimerkiksi radiovastaanotin

ei tiedä tuleeko siihen häiriösäteilyä vastustajan häirintälähettimestä, viestiaseman lähellä olevasta teollisuushallista, tai samaan viestiajoneuvoon asennetusta loisteputkivalaisimesta. Siten asemapaikkojen valinnassa ja järjestelmien suojaamisessa on aina tarkasteltava kokonaisuutta, ei pelkästään vastustajan mahdollisuuksia ja toimintaa. Herkkiä vastaanottimia, kuten elektronisen tiedustelun sensoreita sekä tutka- tai radiolaitteita sisältävissä järjestelmissä on paikalliseen kohinatasoon ja laitteiden keskinäiseen sähkömagneettiseen yhteensopivuuteen kiinnitettävä erityistä huomiota. Sähkömagneettisen yhteensopivuuden varmistaminen on tärkeätä myös oman vaikuttamiskyvyn kannalta: omia häirintäjärjestelmiä ei voida käyttää, jos ne häiritsevät tahattomasti myös omia tärkeitä järjestelmiä: esimerkiksi venäläiset eivät kyenneet aluksi asentamaan uuteen MiG-29 hävittäjäänsä sisäistä omasuoja-häirintäjärjestelmää, koska se häiritsi liikaa koneen omaa avioniikkaa[13].

## Elektroninen taistelukenttä

Nykyaikaisessa taistelussa käytetään niin paljon elektronisia laitteita, että sähkömagneettinen spektri on sotatoimialueella käytännössä täynnä erilaisia lähetteitä. Näiden käsittelyä varten on otettu käyttöön käsite *elektroninen taistelukenttä*. Se käsittää kuvauksen taistelukentällä – tai pikemminkin viisiulotteisessa[d] *taistelutilassa* toimivista järjestelmistä, joihin kuuluvat sekä omat että vastustajan järjestelmät ja näiden lisäksi alueella vaikuttavat kolmansien osapuolten järjestelmät[e]. Vastustajan järjestelmät mielletään sekä elektronisena uhkana että oman elektronisen sodankäynnin maaleina. Armeijakunnan elektronisella taistelukentällä voi olla esimerkiksi

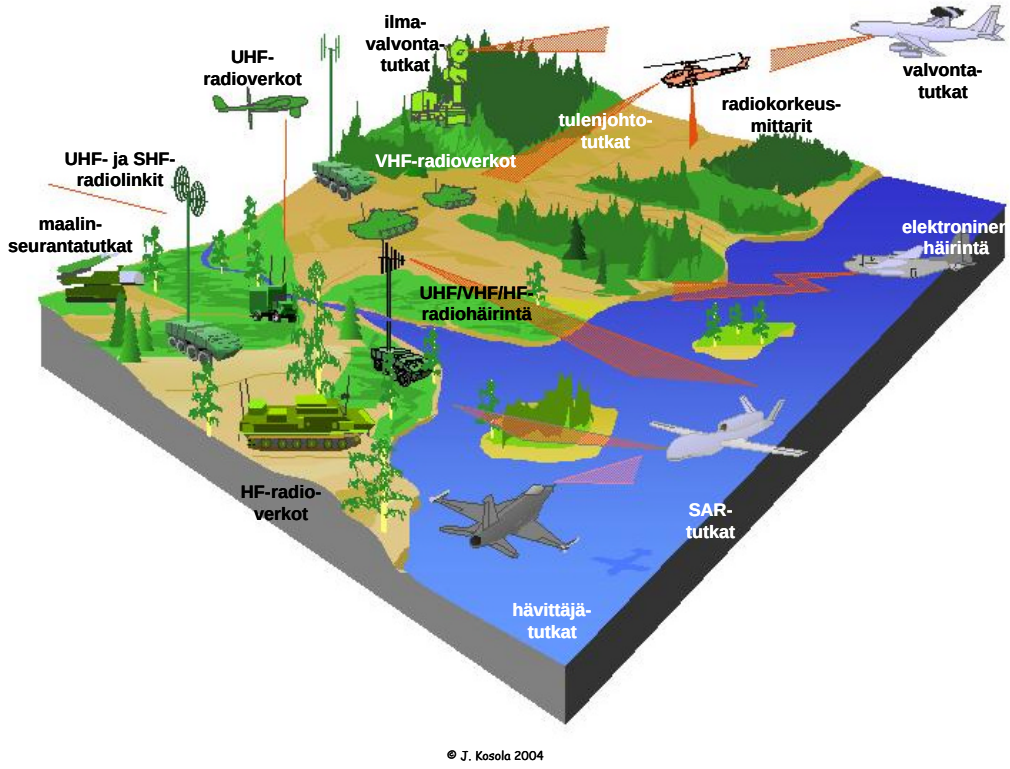
- 2000-4000 VHF-radiota, joista osa hyppivätaajuisia ja osa kiinteätaajuisia
- 300-500 HF-radiota
- 50-100 analogista VHF/UHF-radiolinkkiä
- 200-300 digitaalista UHF/SHF-radiolinkkiä, osa taajuushyppiviä
- 20 troposfäärisirontalinkkiä
- 20-100 satelliittilinkkiä
- 1000-2000 satelliittipaikanninta
- 15-30 vastatykistötutkaa
- 100-200 lentokoneiden, helikoptereiden, ilmatorjuntajärjestelmien tai alusten tulenjohtotutkaa

[d] Taistelukentän viisi ulottuvuutta ovat kolme volyymistä ulottuvuutta sekä sähkömagneettinen spektri (taajuusalue) ja aika.

[e] Käsite ”alueella vaikuttavat kolmansien osapuolten järjestelmät” on varsin laaja. Kolmansiin osapuoliin voidaan katsoa kuuluvan paikalliset siviiliviranomaiset, yritykset ja muut yhteiskunnan toimijat sekä mahdollisesti naapurivaltiot. Lisäksi on huomattava, että sähkömagneettinen spektri ei tunne valtionrajoja: siinä missä korkeimmat taajuudet etenevät vain rajoitetulle alueelle, matalat taajuudet etenevät jopa maapallon laajuisesti. Siten operaatioalueella voi olla lähetteitä hyvinkin kaukaa ja vastaavasti oman toiminnan vaikutus voi ulottua erittäin laajalle alueelle maapallolla ja sen lähiavaruudessa.

- 40-60 maastonvalvonta- ja vastatykistötutkaa
- 50-80 ilma- tai merivalvontatutkaa maassa, aluksissa ja lentokoneissa
- 60-100 pulssidopplertutkaa
- 20-40 rynnäkköpommittajien tai hävittäjien monitoimitutkaa
- 2-5 SAR-tutkaa lentokoneissa, lennokeissa tai satelliiteissa
- 50-100 radiokorkeusmittaria
- sadoista tuhansiin tutkahakupäillä varustettua ohjusta

Armeijakunnan taistelukentällä voi siis toimia 5 000 – 10 000 erilaista järjestelmää, jotka lähettävät informaatiota sähkömagneettiseen spektriin tai ottavat sitä vastaan spektristä. Lukumääriä tarkasteltaessa on kuitenkin huomattava, että vain osa näistä järjestelmistä on samanaikaisesti aktiivisena. Toisaalta spektrissä voi esiintyä miljoonia tutkapulsseja sekunnissa. Edellä kuvatut ovat vain suuntaa antavia lukuja, joiden tarkoituksena on antaa käsitys siitä kuinka paljon aktiviteettia nykyaikaisella elektronisella taistelukentällä saattaa olla. Tarkat käsitykset lähettimien määrästä riippuvat luonnollisesti kriisin ja sodan yleisestä kuvasta sekä taisteluiden vaiheesta ja sijainnista.




**Kuva 4: Esimerkki elektronisesta taistelukentästä toimintaympäristönä.**

Operaatioalueella on edellä kuvattujen järjestelmien lisäksi mitä todennäköisimmin myös lukuisia erilaisia sotilaalliseen käyttöön otettuja siviilijärjestelmiä ja mahdollisesti väestösuojelun, pelastuspalvelun ja yksittäisten siviilihenkilöiden viestijärjestelmiä. Tämän vuoksi sotilaallisten, kaksoiskäyttöisten ja siviilijärjestelmien välistä eroa on vaikeaa ja itse asiassa tarpeetontakin määritellä. Amerikkalaisten kokemusten mukaan taajamaympäristössä toteutettavissa operaatioissa jopa 90% operaatioalueen spektrissä havaittavista tietoliikennesignaaleista on peräisin siviilijärjestelmistä[14].

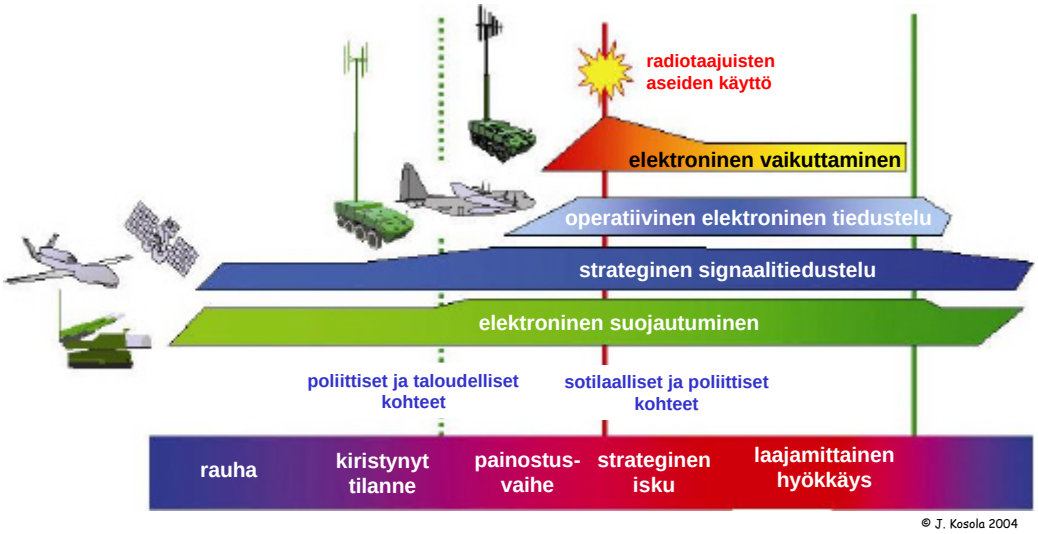
## Elektronisen sodankäynnin rooli sotilasoperaatioissa

Elektroninen sodankäynti (ELSO, engl. Electronic Warfare, EW) tarkoittaa sähkömagneettisen säteilyn hyväksikäyttöä oman sodankäynnin edistämiseen ja vastustajan sodankäyntikyvyn heikentämiseen. Sähkömagneettista spektriä hyväksikäyttävät tiedustelu-, valvonta-, johtamis- ja asejärjestelmät eivät sinänsä ole osa elektronista sodankäyntiä. Elektronisesta sodankäynnistä on kyse silloin, kun sähkömagneettisen spektrin avulla pyritään edistämään tai haittaamaan näiden järjestelmien toimintaa tai silloin kun näistä järjestelmistä pyritään saamaan tietoja sähkömagneettisen spektrin kautta[15]. Puolustusvoimat on määritellyt elektronisen sodankäynnin seuraavasti:

> **Elektroninen sodankäynti (ELSO**, engl. **Electronic Warfare, EW)** on sähkömagneettista säteilyä käyttävien tai lähettävien järjestelmien tiedustelua ja valvontaa ja niihin vaikuttamista sekä suojautumista näiden järjestelmien vaikutuksilta. Elektronisen sodankäynnin tavoitteena on:
>
> **1)** **hankkia passiivisin menetelmin sähkömagneettisen spektrin kautta tietoa** vastustajan joukoista ja järjestelmistä tilannekuvan muodostamiseksi, maalien paikantamiseksi sekä uhkavaroituksen antamiseksi omille joukoille välittömästi uhkaavista vaaroista,
>
> **2)** **lamauttaa ja hidastaa** vastustajan tiedustelua, valvontaa, johtamistoimintaa sekä ase- ja omasuojajärjestelmien käyttöä **häiritsemällä** tai **estämällä** sähkömagneettisen spektrin käyttöä, **harhauttamalla** sensoreita sekä **lamauttamalla** elektronisia järjestelmiä ja
>
> **3)** **suojata** omat joukot ja niiden järjestelmät **estämällä** tai **harhauttamalla** vastustajaa saamasta tietoa niiden määrästä, sijainnista, liiketilasta, käyttötavasta ja -aikeista sekä teknisistä ja toiminnallisista ominaisuuksista sekä **valvomalla** omaa sähkömagneettisen spektrin käyttöä.

Elektroninen sodankäynti on osa sodankäyntiä. Kuitenkin sodan ajan toimintakyky edellyttää varautumista toimintaan jo rauhan aikana. Näkyvin muoto tästä varautumisesta on joukkojen varustaminen, kouluttaminen ja harjoittaminen toimimaan elektronisen taistelukentän toimintaympäristössä. Kaiken tämän perustana toimii

taustalla myös tiedonhankinta vastustajan järjestelmistä ja toimintatavoista sekä omien järjestelmien, joukkojen ja toimintatapojen suojaaminen. Signaalitiedustelu ja muiden tiedustelulajien avulla tehtävä elektronisen sodankäynnin tarpeita palveleva tiedustelu ja muu tiedonhankinta on käynnissä myös syvän rauhantilan aikana, eikä se välttämättä edes näy sen kohteena olevalle valtiolle. Kansainvälisen kriisin lähestyessä tiedonhankintaa tehostetaan ja myös signaalitiedustelun järjestelmien käyttöä lisätään. Tällöin tiedustelu toimii strategisella tasolla pyrkien toisaalta selvittämään kriisin kehittymisen suuntaa ja kehittymisnopeutta ja toisaalta selvittämään vastustajan järjestelmien ja joukkojen ominaisuuksia. Samalla myös elektronisen suojautumisen toimenpiteitä tehostetaan, jotta kyetään varmistumaan järjestelmien toiminnasta mahdollisten taisteluiden alkaessa.




**Kuva 5: Elektronisen sodankäynnin mahdollisia painotuksia kriisin eri vaiheissa.**

Kun päätös taistelutoimien aloittamisesta on tehty, tai kun hyökkäyksen todennäköisyys arvioidaan riittävän suureksi, korostuu operatiivinen elektroninen tiedustelu, jonka tehtävänä on hankkia sotilaallisen operaation suunnittelussa ja järjestelmien ohjelmoinnissa tarvittavat tiedot. Varsinainen elektroninen hyökkäys voi liittyä yhteiskunnan perusrakenteisiin liittyvään vaikuttamiseen tai hyökkäykseen puolustusjärjestelmää vastaan. Elektroninen hyökkäys liittyy siten sekä strategiseen iskuun, että sitä mahdollisesti edeltävään poliittiseen painostukseen.

# ELSO informaatiosodankäynnin työkaluna

## Informaatiosodankäynnin käsite

Käsitteenä informaatiosodankäynti (Information Warfare, IW) on suhteellisen uusi eikä vielä täysin vakiintunut. Puolustusvoimien määritelmän mukaan ***informaatiosodankäynti on valtion yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja***

***toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja tältä suojautumista***. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin strategisella, operatiivisella tai taktisella tasolla. Informaatiosodankäynnissä puolustusvoimat on siten vain yksi toimija muiden tahojen kanssa: valtion kyky käydä informaatiosodankäyntiä ja suojautua sen vaikutuksilta edellyttää aivan uudenlaista yhteistyötä viranomaisten kesken ja yhteiskunnan infrastruktuurista vastaavien tahojen kanssa.

Informaatiosodankäynnin keskeiset vaikuttamis- ja suojautumiskeinot ovat tietoverkkosodankäynti, elektroninen sodankäynti, psykologinen sodankäynti, fyysinen vaikuttaminen tiedustelu-, valvonta- ja johtamisjärjestelmään, operaatioturvallisuus ja harhauttaminen. Informaatiosodankäynnin käsitteen vakiintumattomuuden vuoksi eri maiden asevoimilla on erilaisia määritelmiä ja käsityksiä siitä, mitä informaatiosodankäynti itse asiassa on. Joidenkin näkemysten mukaan se sisältää edellä mainittujen osa-alueiden lisäksi myös tiedottamisen ja siviilisuhteiden hoitamisen, kun taas kapea-alaisimpien näkökulmien edustajat mieltävät sen pelkäksi tietojärjestelmä- ja mediasodankäynniksi, rajoittuneimmillaan jopa synonyymiksi psykologisille operaatioille.

***Informaatiosodankäynti on osa normaalia operatiivista toimintaa.***

Puolustusvoimien informaatiosodankäynnin tavoitteena on turvata informaatiouhan alla valtakunnallisesti elintärkeiden sotilaallisten toimintojen jatkuminen kaikissa valmiustiloissa. Suorituskykytavoitteet saavutetaan parhaiten siten, että informaatiosodankäynti muodostaa kiinteän osan operatiivista suunnittelua ja operaatioiden toteutusta. ***Informaatiosodankäynti ei siis ole erillinen jälkikäteen operaatioon lisättävä osa-alueensa, vaan osa normaalia operatiivista toimintaa***. Sama pätee myös informaatiosodankäynnin osa-alueisiin, erityisesti elektroniseen sodankäyntiin. Jotta elektronisen sodankäynnin kyvystä saadaan olennaista hyötyä, sen on oltava kiinteä osa operatiivisen johdon alaista operatiivista toimintaa.

Informaatioylivoima on suhteellinen ylivoima informaatio-operaatiossa vastustajaan nähden ajantasaisen ja oikean informaation keräämisessä, käsittelemisessä ja jakamisessa sitä tarvitseville. Informaatioylivoima saavutetaan sekä tukemalla omaa informaatioprosessia että heikentämällä vastustajan informaatioprosessia. Informaatiosodankäynnin kannalta teknisen kehityksen painopisteenä tulee olemaan toisaalta oman tilannetietoisuuden lisääminen ja toisaalta vastustajan tilannetietoisuuden vähentämiseen soveltuvat keinot.

Informaation kerääminen ja siirtäminen perustuu taistelukentällä useimmiten sähkömagneettisen spektrin käyttöön. Tämän vuoksi elektroninen sodankäynti kykenee tukemaan operaatioturvallisuutta, psykologisia operaatioita, fyysistä vaikuttamista sekä tietojärjestelmäoperaatioita ja operatiivista harhauttamista. ELSO onkin tämän vuoksi informaatiosodankäynnin keskeisin elementti. On kuitenkin huomattava, että ELSO on informaatiosodankäyntiä laajempi kokonaisuus, mihin sitä ei sen vuoksi saa sulauttaa.

Esimerkiksi seuraavat ELSO:n osa-alueet eivät kuulu informaatiosodankäyntiin:

- asejärjestelmät ja niiden toimintakyvyn varmistaminen tai lamauttaminen
- joukon omasuoja
- lavettien omasuojajärjestelmät


**Kuva 6: Informaatiosodankäynnin osa-alueet puolustusvoimien määritelmän mukaan. Signaalitiedustelu ja sähkömagneettisen spektrin hallinta eivät kuulu elektroniseen sodankäyntiin, mutta tukevat sitä.**

Toisaalta elektronisesta sodankäynnistä voidaan katsoa kuuluvaksi informaatio-operaatioiden piiriin vaikkapa seuraavat alueet:

- elektroninen tilannekuva ja uhkavaroitus
- vastustajan johtamisjärjestelmän häirintä ja harhauttaminen
- tiedustelu-, valvonta- ja maalinosoitusjärjestelmien tuki
- taistelukentän maalintunnistus: omat, viholliset ja neutraalit
- omien omatunnistusjärjestelmien suojaaminen ja vastustajan järjestelmien lamauttaminen
- navigointi- ja paikantamisjärjestelmien suojaus, häirintä ja lamauttaminen

Kategorista jakoa siitä, mikä osa ELSO:sta kuuluu informaatiosodankäyntiin ja mikä jää sen ulkopuolelle ei ole mielekästä eikä tarpeellistakaan tehdä.

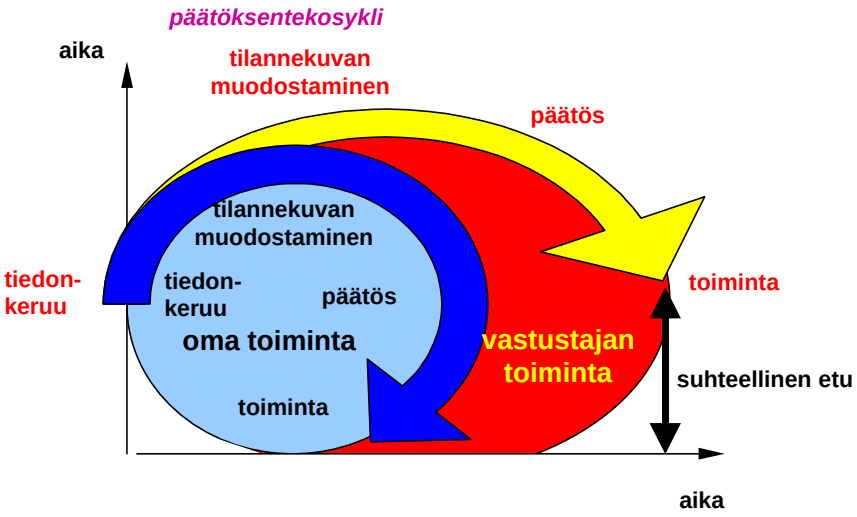
## Informaatio-operaatiot

Informaatio-operaatio (Information Operation, IO) on puolustusvoimien määritelmän mukaan *informaatiosodankäynnin osa-alueisiin perustuva sotilas- ja/tai siviili-ioperaatio*. Kyseessä voi siis olla kokonaan sotilasvoimin tehtävä operaatio, täysin siviilien toimeenpanema operaatio tai sotilas- ja siviiliviranomaisten yhteistyössä suunnittelema ja toimeenpanema operaatio, jossa käytetään yhtä tai useampaa informaatiosodankäynnin osa-aluetta tiedonkeruuseen, suojautumiseen tai vaikuttamiseen. Informaatio-operaation määritelmä on niin väljä, että se kattaa tarvittaessa lähes kaiken sotilaallisen toiminnan, muttei kuitenkaan rajoitu sotilas-toimintaan, vaan voi sisältää esimerkiksi poliittisia tai tiedotuksellisia toimia.

Informaatio-operaatio voi olla puolustuksellinen tai hyökkäyksellinen ja se vastaa yleensä johonkin informaatiouhkaan. ***Informaatiouhka on tahtoon, tietoon ja tietoa käsitteleviin henkilöihin ja järjestelmiin kohdistuvaa tahallista tai tahatonta toimintaa, joka voi heikentää informaation luotettavuutta, luottamuksellisuutta, eheyttä tai käytettävyyttä sekä ohjata mielipiteen muodostusta ja päätöksentekoa vastustajan haluamaan suuntaan erilaisin tietoteknisin, sähkömagneettisin, fyysisin tai psykologisin keinoin***. Informaatio-operaation kohteena voi olla esimerkiksi oma kansa, omat sotilasjoukot, vastustaja kansakuntana, vastustajan sotilaallinen voima, sodan ulkopuolella oleva valtio tai vaikkapa tiedostusvälineet. Informaatiosodankäynti kokonaisuutena ja informaatio-operaatiot strategisella tasolla ovat selkeästi tämän kirjan aihepiirin ulkopuolella. Kirjassa keskitytään tarkastelemaan elektronisen sodankäynnin roolia informaatio-operaatioiden toteuttamisessa ja informaatiouhkilta suojautumisessa.

Sodankäynnissä informaatio-operaation tavoitteena voi olla ***johtamisylivoiman*** saavuttaminen vastustajasta. Siinä pyritään nopeuttamaan, varmistamaan ja suojaamaan oma johtamistoiminta sekä hidastamaan vastustajan johtamistoimintaa niin, että vastustaja kykenee tekemään päätöksiä ja toimeenpanemaan niitä huomattavasti hitaammin. Tällöin vastustaja tekee päätöksensä vanhoilla ja puutteellisilla sekä mahdollisesti jopa väärillä tiedoilla ja paikkaansa pitämättömillä olettamuksilla. Kun vastustajan päätökset alkavat vaikuttaa joukkojen siirtoina, tiedustelun kohdentamisena tai tulivalmisteluina, tilanne on jo muuttunut, eikä vastustajan toimenpiteistä ole sen kaavailemaa hyötyä. Kuvassa 7 on esitetty johtamis-ylivoiman muodostuminen oman ja vastustajan johtamisprosessin nopeuseroista. Englanninkielisissä lähteissä puhutaan **OODA**-silmukasta[16] päätöksenteon vaiheiden mukaisesti:

- **O**bserve – kerää tiedot
- **O**rientate – muodosta tilannekuva
- **D**ecide – tee päätös
- **A**ct – pane päätös toimeen




**Kuva 7: Johtamisylivoiman hankkiminen perustuu oman johtamissyklin nopeuttamiseen ja varmistamiseen sekä vastustajan johtamisen hidastamiseen ja harhauttamiseen. Suhteellinen etu kuvaa sitä aikaetua, joka tällä saavutetaan. Kun etu on riittävä, voidaan saavuttaa tilanne, jossa vastustaja toimii vanhan ja väärän tiedon perusteella.**

Asioiden välistä vuorovaikutussuhdetta kuvaava OODA-silmukka pätee periaatteessa niin operatiivisen päätöksenteon kuin vaikkapa asejärjestelmien toiminnan kuvaamiseen. Se on kuitenkin voimakkaasti yksinkertaistettu malli, joka ei ota huomioon samanaikaista rinnakkaista toimintaa, jollaista esimerkiksi taistelun johtaminen todellisuudessa on. Pelkistettynä malli soveltuu kuitenkin hyvin toiminnan perusajatuksen pohjaksi.

## Vaikutuspohjainen maalitus

Sodankäynnissä vastustajaan vaikutetaan niillä välineillä, jotka kulloinkin ovat käytettävissä. Tekninen kehitys on muuttanut käytettävän välineen käsitettä ja sisältöä. 1800-luvulla välineen piti yleensä olla äänen kantaman sisäpuolella ja maalin näköyhteydellä. 1900-luvulla viestitekniikan kehitys mahdollisti tulipyyntöjen välittämisen myös kuuloetäisyyden ulkopuolelle. 2000-luvulla sensorijärjestelmien kehitys mahdollistaa lähes koko taistelutilan valvonnan pinnasta, ilmasta ja avaruudesta kaikilla sähkömagneettisen spektrin kaistoilla näkyvän valon alueelta infrapuna-, tutka- ja radiotaajuuksille. Tieto- ja tiedonsiirtotekniikan kehitys mahdollistaa sensoreiden antaman tiedon keräämisen ja edelleen välittämisen reaaliaikaisesti tai lähes reaaliaikaisesti koko taistelukentän alueelle. Tällöin komentajat ja taistelunjohtajat kykenevät havaitsemaan, seuraamaan ja tunnistamaan joukkoja ja järjestelmiä tosiaikaisesti myös ilman välitöntä kosketusta vastustajaan. Asejärjestelmien kantaman kasvaminen ja ohjautustekniikoiden kehittyminen puolestaan mahdollistaa sen, että havaittuihin maaleihin voidaan käyttää tilanteen,

tarpeen, maalityypin, haluttavan vaikutuksen ja oman toiminta-ajatuksen mukaan soveliasta asejärjestelmää. Keskeistä on määritellä, mikä on asejärjestelmän käytöltä haluttu vaikutus: Onko kohde tuhottava tai lamautettava, vai riittääkö, että sen halu tai kyky osallistua taisteluun estetään? Keino tulee valita tämän mukaisesti. Jos tavoitteena on vastustajan tuhoaminen, se voidaan parhaiten tehdä fyysisellä vaikuttamisella, siis perinteisin asein. Jos taas tavoitteena on vastustajan toiminnan lamauttaminen, voidaan keinona käyttää:

- Fyysistä vaikuttamista: eliminoidaan vastustajan keskeiset johtajat ja/tai asiantuntijat, tuhotaan sen keskeiset tiedustelu- ja valvontajärjestelmän, johtamisjärjestelmän tai asejärjestelmän solmupisteet tai estetään niiden liike täsmäasein, epäsuoralla tulella, tuliylläköin, suluttamalla tms. konventionaalisella voimankäytöllä.
- Operaatioturvallisuutta yhdistettynä operatiiviseen harhauttamiseen: vastustajan järjestelmä toimii sinänsä oikein, mutta vastustajan komentaja tekee vääriä päätöksiä: jättää hyökkäämättä, hyökkää liian aikaisin tai liian myöhään, siirtää painopistettään väärään paikkaan jne.
- Elektronista sodankäyntiä: vastustaja ei kykene muodostamaan tilannekuvaa tai muodostaa väärän käsityksen tilanteesta, vastustaja ei kykene johtamaan joukkojaan eikä käyttämään epäsuoraa tulta tai ilmatorjuntaa jne.
- Tietojärjestelmäsodankäyntiä: vastustajan keskeiset tietojärjestelmät lamautuvat kriittisellä hetkellä.
- Psykologista sodankäyntiä: vastustajan johtajat saadaan epäröimään ja tekemään huonoja tai jopa vääriä päätöksiä, joukkojen taistelumoraali laskemaan jne.

Tyhjentävää luetteloa vaikutuspohjaisen maalituksen kohteista, keinoista ja vaikutusmahdollisuuksista ei ole mahdollista eikä järkevääkään antaa, sillä ne ovat aina tilannesidonnaisia. Olennaista on kuitenkin integroida kaikkien vaikuttamis-järjestelmien maalitusprosessi sekä tehdä maalitus tiedustelu- ja valvontajärjestelmän antaman tilannekuvan ja komentajan taisteluajatuksen perusteella. Esimerkiksi USA:n ilmavoimien ajatuksena on integroida ilma-, avaruus- ja informaatiosodankäynnin menetelmät ja prosessit yhdeksi kokonaisuudeksi, jossa välineet tukevat ja korvaavat toisiaan halutun vaikutuksen aikaan saamiseksi[17]. Maalitus voidaan vaiheistaa esimerkiksi seuraavasti[18]:

1. Päätetään haluttu vaikutus vastustajan toiminnalle oman operaation aikana. Tällöin on kyettävä tarkastelemaan asiaa myös seurannaisvaikutusten kannalta[19].

2. Päätetään toimenpiteen haluttu vaikutus omalle toiminnalle tai määritetään mitä sivuvaikutuksia voidaan kestää.

3. Päätetään mihin vaikutetaan: Vaikutetaanko tahtoon (johtajat ja joukot), suorituskykyyn (joukot ja järjestelmät) vaiko toiminta-ajatukseen (suunnitelmat ja käskyt sekä niiden toimeenpano).

4. Päätetään millä elementillä, tai minkä elementtien yhteiskäytöllä, vaikutetaan sekä koska ja miten vaikutus toteutetaan.

5. Päätetään miten eri elementit synkronoidaan yhteisoperaatiossa.

Elektroninen sodankäynti on harvoin ainoa valittava vaikutuskeino, mutta sen pitäisi olla lähes jokaisessa tapauksessa yksi osa kokonaisratkaisua. Seuraavassa esitetään elektronisen sodankäynnin mahdollisuuksia tukea muita vaikuttamisen elementtejä.

## ELSO fyysisen vaikuttamisen tukena

Elektronisella sodankäynnillä voidaan käytettävissä olevien elektronisten vaikuttamis-järjestelmien sen salliessa esimerkiksi:

- Paikantaa vastustajan komentopaikat, tuliasemat ja reservien sijainti oman tykistön maaleiksi sekä partiotiedustelun ja iskuosastojen suuntaamiseksi.
- Lamauttaa vastustajan johtamisyhteydet murtoalueella hyökkäyshetkellä, jolloin se ei kykene johtamaan tulta, käynnistämään vastahyökkäystä eikä käyttämään reservejään ajoissa.
- Lamauttaa määräajaksi vastustajan ennakkovaroitus- ja omasuojajärjestelmät, jolloin omien aseiden vaikuttavuus kasvaa.
- Lamauttaa, häiritä ja harhauttaa vastustajan tiedustelu- ja valvonta-järjestelmä määräajaksi, mikä estää vastustajan tiedustelutulijärjestelmän toiminnan ja operatiivisen tulenkäytön omaan syvyyteemme ja siirtymis-reiteille.
- Tuottaa arvioita tulen osuvuudesta ja asevaikutuksen aiheuttamista tappioista vastustajalle (BDA, Battle Damage Assessment), minkä perusteella voidaan päätellä tuleeko tulenkäytön suoritus, oli se sitten tykistön isku tai vaikkapa lentorynnäkkö, uusia.

Elektronisen sodankäynnin tekniikoita käytetään myös konventionaalisissa aseissa. Esimerkkinä voidaan mainita vaikkapa tutkasäteilyyn hakeutuvat ohjukset (ARM – Anti-Radiation Missile), joita on ollut jo pitkään operatiivisessa käytössä. Tulevaisuudessa vastustajan elektronisiin järjestelmiin hakeutuvat ammukset voivat yleistyä. Tällaisia voisivat olla esimerkiksi radio- tai tutkasäteilyyn hakeutuvat kranaatinheittimen ammukset[20].

Elektronisella sodankäynnillä voidaan myös suojata joukkoja ja järjestelmiä vastustajan fyysiseltä vaikuttamiselta. Suurvalta-armeijoissa on pyrkimyksenä lähitaistelun välttäminen ja vastustajan tuhoaminen tulella. Tämä hoidetaan massiivisella tulenkäytöllä, josta esimerkiksi venäläiset käyttävät nimitystä

*rakenteellisen tuhoamisen menetelmä*[21]. Tulenkäytön järjestäminen ei enää perustu taistelujoukon suorituksiin, vaan kaukovaikutteisten aseiden käyttämiseen, jolloin tulenjohtajan ja asejärjestelmän välinen etäisyys kasvaa tehden näiden välisen kommunikoinnin haavoittuvammaksi vastatoimille[22,f]. Tulenkäytöllä pyritään tuhoamaan paitsi vastustajan joukot, ennen kaikkea sen edellytykset jatkaa taistelua, ja siinä siirrytään käyttämään kasvavassa määrin täsmäaseita[23]. Elektroninen sodankäynti mahdollistaa joukon suojautumisen vastustajan fyysiseltä tulenkäytöltä useilla eri tavoilla. Hyökkääjän siirtyessä käyttämään organisaatioihin kuuluvien ja joukkojen välittömänä tukena olevien tuliyksiköiden sijasta koko yhtymää tukevia kaukovaikutteisia aseita, joutuu sen maalinosoitus- ja tulenkäytön järjestelmä tukeutumaan sähkömagneettisen spektrin laajamittaiseen käyttöön. Jos se kiistetään, järjestelmä ei toimi. Esimerkiksi venäläisen tykistön toiminta vastustajan syvyyteen perustuu suurelta osin maalien paikantamiseen lennokki- ja lentotiedustelulla ja muilla teknisillä tiedusteluvälineillä (ml. elektronisen tuen sensorit) sekä tulen johtamiseen (maaston-valvonta- ja vastatykistö)tutkilla, joten näiden toiminnan häiritseminen tai lamauttaminen estää suurelta osin tykistöaseen käytön syvyyteen[24]. Toinen merkittävä suojautumismahdollisuus muodostuu elektronisen sodankäynnin kyvystä kiistää täsmäaseiden toimintakyky.

## ELSO operaatioturvallisuuden tukena

Elektroninen tuki kykenee valvomaan omaa sähkömagneettisen spektrin käyttöämme ja havaitsemaan mikäli omat joukot lähettävät spektriin jotakin sellaista, jonka vastustajakin voi havaita. Tällöin voidaan ohjata omien johtajien ja joukkojen toimintaa ja kehittää operaatioturvallisuusajattelua ja -osaamista joukoissa. Elektronisen tuen avulla voidaan myös tarkkailla havaitsiko vastustaja oman lähetteemme ja miten se tähän reagoi. Siten elektronisen sodankäynnin keinoin voidaan tukea arviota operaatioturvallisuustilanteen kehittymisestä. Käytettävissä olevista järjestelmistä riippuen elektronisen sodankäynnin keinoin voidaan myös estää vastustajan tiedustelu- tai erikoisjoukkoja tai ilmatulenjohtajia välittämästä viesti-välinein sellaisia tietoja, jotka vaarantavat operaatioturvallisuuden[g].

---

[f] Ensimmäinen elektronisen häirinnän soveltaminen sotilasoperaatiossa toteutettiin ilmeisesti venäläisten häiritessä japanilaisten alusten tulenjohtoa Japanin-Venäjän sodassa 1904. Japanilaiset johtivat Port Arthurin pommituksen tulenjohdon läheltä tähystäviltä risteilijöiltä kauempana sijaitseville taistelulaivoille radioviestityksellä. Venäläisten mukaan radiohäirinnän vuoksi käytännössä tähystämättömänä suoritettu tulitus ei johtanut juuri minkäänlaisiin venäläistappioihin.

[g] Operaatioturvallisuuden valvonta elektronisen tuen avulla ja tarvittaessa vahvistaminen elektronisen vaikuttamisen voimin voi olla keskeinen tekijä taistelun onnistumisen kannalta. Tästä on hyvänä esimerkkinä Tsushiman meritaistelu 1905, joka päätyi Venäjän Itämeren laivaston tuhoon. Japanilaiset olivat aiemmin paikantaneet venäläisten alukset ja paljastaneet operaatioajatuksen venäläisten heikon radiokurin vuoksi. Sen vuoksi venäläiset käyttivät radiohiljaisuutta päästäkseen Tsushiman salmen läpi japanilaisten huomaamatta. Japanilaisten partio kuitenkin havaitsi venäläisalukset ja viestitti radiolla alusosaston liikkeistä. Venäläiset olisivat voineet estää japanilaisaluksen tiedustelutietojen välittämisen elektronisella häirinnällä, ja siten viivästyttää japanilaisten vastatoimia niin, että venäläiset olisivat päässeet salmen läpi...

## ELSO operatiivisen harhauttamisen tukena

Elektronisen sodankäynnin keinoin voidaan paikantaa vastustajan sensorit, joita pyritään harhauttamaan ja muodostaa käsitys vastustajan tiedustelu- ja valvontajärjestelmästä sekä päätöksentekoon liittyvistä komentosuhteista harhautuksen perusajatuksen muodostamiseksi. Vastustajan sensoreiden analysoimisen perusteella voidaan tukea harhautusoperaation suunnittelua ja ohjata sopivien harhautusvälineiden valintaa ja mahdollista tilapäisvälineiden tarkoituksenmukaista valmistusta. Näin harhauttamisella voidaan antaa yhdenmukainen kuva niillä sähkömagneettisen spektrin alueilla (näkyvä valo, ultraviolettisäteily, lämpösäteily ja radiotaajuiset herätteet), joilla vastustaja kykenee toimintamme havaitsemaan. Mikäli se havainnoi harhautuksemme jollakin näistä, muttei saa varmistusta jollakin toisella menetelmällä, koko harhautusoperaatio voi valua hukkaan.

Elektronista harhauttamista voidaan käyttää tukemaan yhtymän operaation toimintaajatukseen kuuluvaa harhauttamista. Vastustajaa voidaan harhauttaa elektronisesti esimerkiksi:

- luomalla valelähetteitä erilaisilla emulaattoreilla, jotka antavat kuvan siitä, että kyseessä onkin jonkinlainen järjestelmä tai joukko, jota todellisuudessa ei ole olemassa.
- luomalla todellisilla järjestelmillä harhakuva joukon toiminnasta, sijainnista, liikkeestä tai painopisteestä
- antamalla vastustajan siepata johtamissanomia, joiden sisältö tukee harhautuksen uskottavuutta.

Lennokkeihin tai ilmasta pudotettaviin vapaasti liitäviin harhamaaleihin tai raketti- tai suihkumoottorilla lentäviin harhaohjuksiin asennetuilla valemaalilähettimillä voidaan matkia hävittäjän tai rynnäkkökoneen tutka-, radio- ja lämpöherätettä. Näillä pakotetaan vastustaja valitsemaan käynnistääkö torjuntatoimet – aktivoidako tutkat ja ampua ohjukset – vaiko ei. Ensimmäisessä vaihtoehdossa puolustaja paljastaa taktiikkansa ja tutkaverkkonsa, asettaa sen alttiiksi tutkasäteilyyn hakeutuville ohjuksille ja tuhlaa arvokkaat ohjuksensa arvottomiin valemaaleihin. Jälkimmäisessä tapauksessa puolustaja puolestaan asettaa ilmatorjunnalla suojattavan kohteen alttiiksi ilmahyökkäykselle. Harhamaalin hinta voi olla tuhannesosa sillä suojattavan hävittäjä- tai rynnäkkökoneen hankintahinnasta.

Käytettävissä olevan häirintävoiman mukaisesti voidaan myös tarvittaessa sokaista sellaiset vastustajan sensorit, joita ei kyetä harhauttamaan, tai lamauttaa niiden viestiliikenne. Lisäksi elektronisen vaikuttamisen järjestelmiä voidaan usein käyttää myös varsinaiseen harhautustoimintaan.

---

…Radiohiljaisuuden murtaminen operaatiokäskyn vastaisesti oli kuitenkin liian iso päätös venäläisosaston johdolle.

## ELSO psykologisen operaation tukena

Elektronisen tiedustelun avulla voidaan kerätä vastustajan organisaatiosta, toiminnasta ja johtajien persoonallisuuksista tietoja, joita voidaan edelleen hyödyntää psykologisen sodankäynnin kohderyhmien määrittelyssä ja teemojen suunnittelussa.

Elektronisen sodankäynnin välineitä voidaan käyttää myös psykologisen operaation toteuttamisessa, josta esimerkkinä voidaan mainita amerikkalaisten toteuttama Kuubaan kohdistettu psykologinen vaikuttaminen EC-130E Commando Solo ja EC-130H Compass Call -koneilla[25]. Myös Irakiin kohdistettiin psykologista vaikutusta vastaavilla menetelmillä vuosien 1991 ja 2003 sodissa. Psykologinen vaikuttaminen voidaan toteuttaa esimerkiksi siten, että ensin varmistetaan oman lähetyksen kuuluminen lamauttamalla elektronisesti tai fyysisesti kohteen voimakastehoiset päälähettimet, jonka jälkeen (mahdollisesti valtakunnan rajan ulkopuolelta) ilmasta toteutettu häirintä tai psykologisen teeman sisältävä informaatio saadaan välitettyä kohdemaan radio- tai TV-vastaanottimiin. Tämä voidaan toteuttaa joko erityisillä PSYOP-koneilla (esim. amerikkalaisten Commando Solo) tai häirintäkoneilla (esim. Compass Call), jolloin häirintäsignaalina käytetään PSYOP-nauhoitetta. ELSO:lla voidaan tarvittaessa myös häiritä vastustajan PSYOP-lähetteitä. Tällä voidaan tukea omaa psykologista suojautumista, heikentää vastustajan psykologisia suojautumis-toimenpiteitä sekä estää tätä vaikuttamasta psykologisesti johonkin kolmanteen tahoon.

ELSO-järjestelmillä kyetään kuuntelemaan psykologisen vaikuttamisen kohteena olevia johtajia ja päättelemään heidän keskusteluistaan ja reaktioistaan psykologisen operaation onnistumisastetta ja operaation toteutuksessa tarvittavia muutoksia, esim. teeman tai kohderyhmän vaihtaminen. Lisäksi kuuntelemalla voidaan saada ennakkovaroitus vastustajan tulevista psykologisista operaatioista.

## ELSO tietojärjestelmäsodankäynnin tukena

Elektronisen sodankäynnin keinoin voidaan tukea tietojärjestelmien suojaamista ja niihin vaikuttamista tuottamalla tietoa vastustajan järjestelmien tekniikasta sekä tietojärjestelmien käytöstä kuuntelemalla vastustajan viestiliikennettä. Kuuntelu-tiedustelulla voidaan lisäksi arvioida tietojärjestelmähyökkäyksen vaikuttavuutta ja säätää hyökkäystä sen mukaan, miten vastustaja reagoi siihen. Elektronisella sodankäynnillä voidaan lisäksi lamauttaa tietojärjestelmien varayhteyksiä sekä radio-verkkoja, mikä voi hidastaa vastustajan kykyä toipua tietojärjestelmähyökkäyksestä.

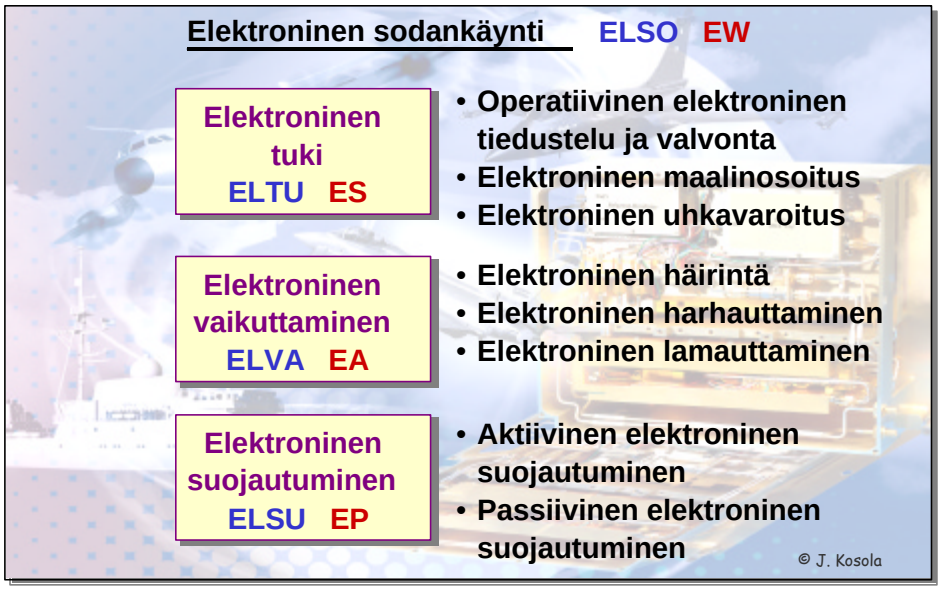
Teknisen kehityksen myötä yhä useammat tietojärjestelmät muuttuvat langattomiksi, mikä lisää elektronisen sodankäynnin aiheuttamia uhkia ja mukanaan tuomia mahdollisuuksia myös tietojärjestelmäsodankäynnissä. Elektronisen sodankäynnin keinoin voidaan tuottaa tietojärjestelmäsodankäynnin joukoille yhteys vastustajan informaatiojärjestelmään sekä häiritä ja lamauttaa tietojärjestelmän toimintaa ja muuttaa järjestelmässä välitettävän tiedon sisältöä.

# 2. ELEKTRONISEN SODANKÄYNNIN ELEMENTIT

Elektroninen sodankäynti jakautuu

1. elektroniseen tukeen
2. elektroniseen vaikuttamiseen
3. elektroniseen suojautumiseen

Elektroniseen sodankäyntiin liittyy lisäksi elektronisen tiedustelun muodossa signaalitiedustelu (SIGINT, Signals Intelligence), jota ei yleensä lueta osaksi ELSO:a, vaan strategista tiedustelua. Signaalitiedustelulla kerätään kuitenkin tietoja myös elektronisen sodankäynnin tarpeisiin. Signaalitiedustelussa käytetään samoja menetelmiä ja osin jopa samoja järjestelmiä kuin elektronisessa tiedustelussa ja valvonnassa, joten sen ryhmittäminen ELSO:n ulkopuolelle kuvaa pikemminkin asioiden organisoimista ja tiedon hyödyntämiskohdetta kuin asian teoreettista tai konseptuaalista olemusta.

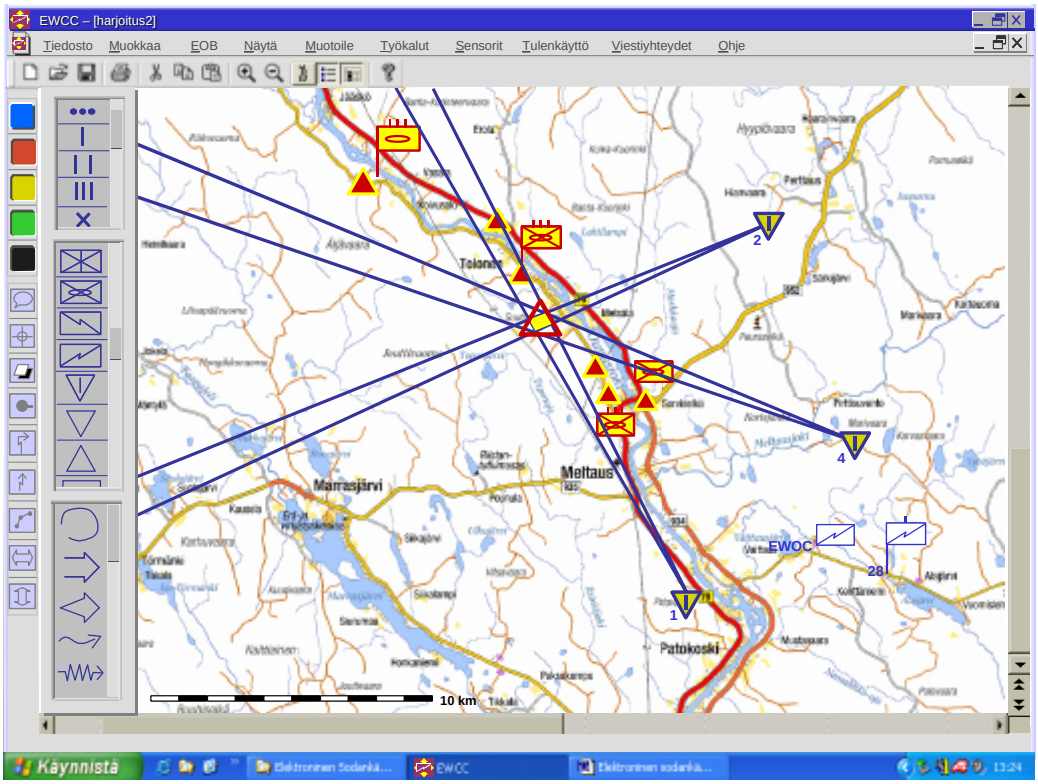



**Kuva 8: Elektronisen sodankäynnin osa-alueet suomalaisten määritelmien mukaisesti.**

Elektronisen sodankäynnin menetelmiä ja tekniikoita käytetään lähes kaikissa taistelukentän järjestelmissä, vaikka ne eivät olisikaan elektronisen sodankäynnin järjestelmiä. Esimerkiksi tutka ei ole ELSO-järjestelmä, vaikka käyttääkin elektronisen sodankäynnin keinoja suojautumiseen. Juuri elektroninen suojautuminen koskee kaikkia järjestelmiä, kun taas elektroninen tuki ja elektroninen vaikuttaminen ovat toiminteita, jotka toteutetaan nimenomaan ELSO-järjestelmissä.

## Elektroninen tuki

Elektroninen tuki (ELTU, engl. Electronic Support, ES**)** on elektronisen sodankäynnin keskeisin elementti. Se havaitsee sensoreillaan taistelukentällä aktiiviset lähettimet, kuten radiolaitteet, tutkat ja radiokorkeusmittarit. Paikantamalla lähettimet se tuottaa reaaliaikaista tilannekuvaa sekä vastustajan että omien järjestelmien sijainnista, liikkeestä ja käytöstä. Elektroninen tuki kykenee muodostamaan tilannekuvan, josta käy ilmi aktiivisesti toimivat omat ja vastustajan joukot sekä taistelualueella mahdollisesti olevat muut toimijat. Elektronisen tuen avulla voidaan päätellä vastustajan joukkojen käytön painopiste, joukkojen suuntautuminen ja arvioitu toiminta. Elektronisen tuen joukot ovat vain yksi osa yhtymän ja ylemmän johtoportaan tiedustelu- ja valvontakykyä ja niiden tuottamia tietoja voidaan täydentää ja tarkentaa muilla tiedustelukeinoilla – ja toisin päin.




**Kuva 9: Elektroninen tuki kykenee muodostamaan reaaliaikaisesti tilannekuvaa yhtymän alueelta paikantamalla ja tunnistamalla vastustajan aktiiviset radio-, tutka- yms. lähettimet. Yksittäinen sensori ei yleensä kykene mittaamaan etäisyyttä maaliin – ainoastaan suunnan – mutta yhdistämällä yksittäiset *suuntimat,* saatu ristisuuntima paljastaa maalin sijainnin. Tämä edellyttää sensoreiden lisäksi myös riittäviä sensoreita yhdistäviä viestiyhteyksiä ja elektronista tilannekuvajärjestelmää.**

Puolustuksessa elektroninen tuki mahdollistaa vastustajan hyökkäyksen rakenteen, aikautuksen ja painopisteen selvittämisen taistelukosketuksesta alkaen. Sillä tuotettuja tietoja voidaan käyttää esimerkiksi panssarintorjunnan ja oman epäsuoran tulenkäytön painopisteiden muodostamiseen. Sen antamien maalitietojen perusteella voidaan johtaa epäsuoraa tulta vastustajan johtamispaikkoja ja tuliyksiköitä vastaan. Aiemmin elektronisesta tuesta on käytetty nimitystä elektroniset tukitoimet (ESM, Electronic Support Measures), joka edelleenkin on osin käytössä.

Elektronisen tuen järjestelmät ovat periaatteessa passiivisia, joten niiden olemassaolo, sijainti tai käyttö ei paljastu vastustajalle[h]. Siten vastustajan on erittäin vaikea havaita ja tuhota tai kiertää niitä. Vastustajan rynnäkkökoneet eivät esimerkiksi havaitse olevansa passiivisen sensorin seurannassa eivätkä siten osaa käynnistää vastatoimenpiteitä. Passiivisen järjestelmän avulla voidaan johtaa tulta suoraan tai ohjata aktiivisia sensoreita siten, että niiden ei tarvitse pitää lähettimiään päällä kuin vain hetkittäin. Tällöin vastustajan on hankalampi havaita ja tuhota niitä.

Elektronisen tuen etuna on se, että tilannekuva syntyy hyvin nopeasti taistelukosketuksen jälkeen, kun joukot käynnistävät aktiiviset sensorinsa ja radiolaitteensa. Samalla saadaan nopeasti paikannettua myös omat joukot sekä seurattua niiden liikkumista ja taistelua reaaliaikaisesti.

Passiivisuus on toisaalta heikkous, sillä elektroninen tuki ei havaitse järjestelmiä ja joukkoja, jotka eivät lähetä mitään sähkömagneettiseen spektriin. Operaatioturvallisuuden ylläpitämiseksi joukot pyrkivät noudattamaan radiohiljaisuutta taistelukosketukseen saakka, jonka jälkeen tulikomentoliikenne, maalinosoitus ja taistelun johtaminen edellyttävät lähetinten käyttöä. Siten tyydyttävää tilannekuvaa ei pelkästään elektronisen tuen keinoin välttämättä saada ennen taistelukosketusta. Toisaalta taistelukosketuksen jälkeen tilannekuva saadaan muodostettua erittäin nopeasti. Lisäksi esimerkiksi hävittäjä- ja rynnäkkökoneosasto ei välttämättä voi toimia ilman aktiivisia lähettimiä; kuten radiokorkeusmittareita, yhteyttä taistelunjohtoon, tai hävittäjä- tai pommitustutkaa. Myöskään tiedustelu- tai tulenjohto-osasto ei voi toimia pelkästään passiivisesti.

Elektroninen tuki on yleensä tärkeimpiä komentajan käytössä olevia sensoreita. Tämän vuoksi vastustajan elektronisen tuen järjestelmän lamauttamiseksi ja oman ELTU-järjestelmän suojaamiseksi on pyrittävä tekemään kaikki mahdollinen. Elektroninen tuki voidaan jakaa sen tuottamien tietojen käyttötarkoituksen perusteella operatiiviseen elektroniseen tiedusteluun ja valvontaan, elektroniseen maalinosoitukseen ja elektroniseen uhkavaroitukseen. Edellä kuvatut toiminteet toteutetaan yleensä samoilla sensoreilla, joiden tuottamaa tietoa vain käytetään eri tarkoituksiin.

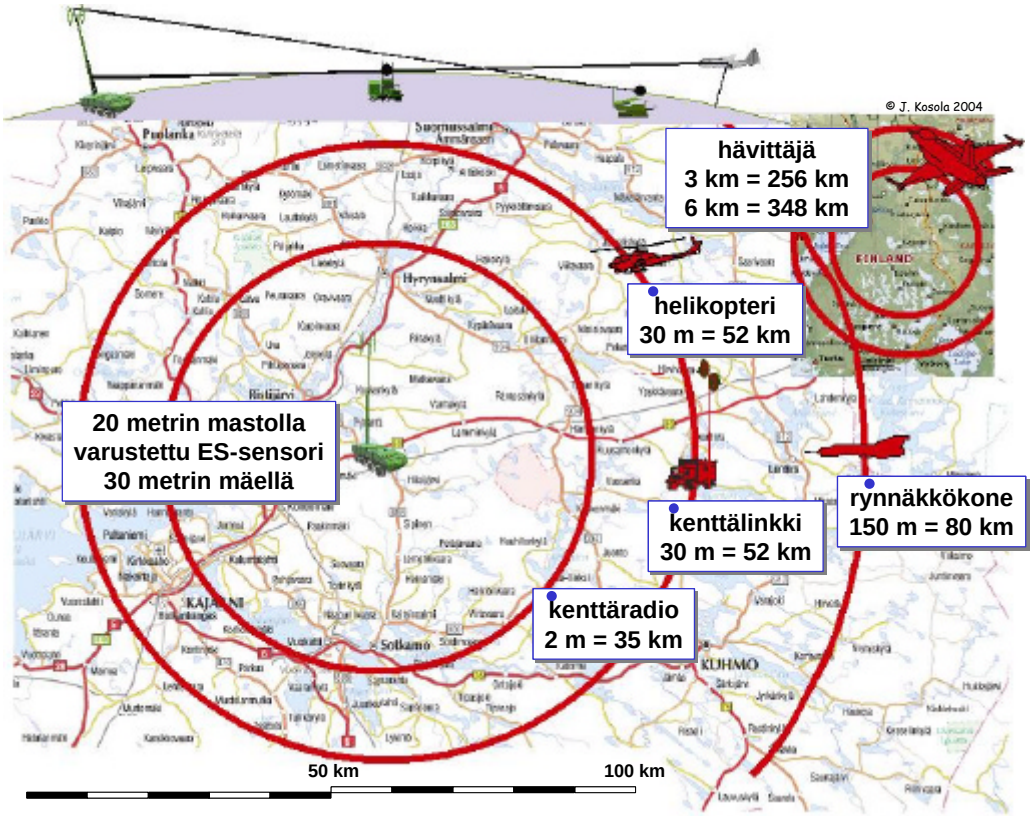
[h] Vaikka elektronisen tuen sensorit perustuvat passiiviseen tekniikkaan, näissä järjestelmissä voi olla käytössä myös tiedonsiirtolaitteita, kuten radiolinkkejä, yhteysradioita tms. lähettimiä, jotka säteilevät sähkömagneettiseen spektriin. Tällä saavutetaan hyvä liikkuvuus ja nopea toiminnan aloittaminen siirron jälkeen uudella toimipaikalla, mutta samalla voidaan menettää sensorin passiivisuuden mukanaan tuoma etu. On toki muistettava, että passiivinenkin asema voi paljastua muilla tiedustelumenetelmillä.

**Kuva 10: Elektronisen tuen kuuntelutiedustelujärjestelmän suuntimoasema, jolla voidaan määrittää suunnat aktiivisiin lähettimiin. Mittaustarkkuuden ja -etäisyyden parantamiseksi suuntimon antenni pitää nostaa mahdollisimman ylös, ainakin kasvillisuuden ja maastoesteiden yläpuolelle. Maston huipussa on viesti-suuntimoissa yleinen ns. Adcock-antenniryhmä, jonka avulla kyetään määrittämään mistä suunnasta siepattava signaali tulee.** [ewation GmbH/MRCM]

## Operatiivinen elektroninen tiedustelu ja valvonta

Operatiivinen elektroninen tiedustelu ja valvonta on vastustajan, omien joukkojen ja mahdollisten kolmansien osapuolten sensori-, navigointi- ja viestijärjestelmiin kohdistuvaa tiedustelua ja valvontaa, jonka tavoitteena on reaaliaikaisen elektronisen tilannekuvan luominen ja ylläpito sekä elektronisen maalinosoituksen ja uhka-varoituksen tukeminen. Elektroninen tiedustelu ja valvonta kykenee taistelukentän aktiivisia lähettimiä, kuten radio- ja tutkalaitteita, havaitsemalla, paikantamalla ja tunnistamalla muodostamaan muutamissa sekunneissa tilannekuvan, josta käy ilmi

aktiivisesti toimivat omat ja vastustajan joukot sekä taistelualueella mahdollisesti olevat muut toimijat.

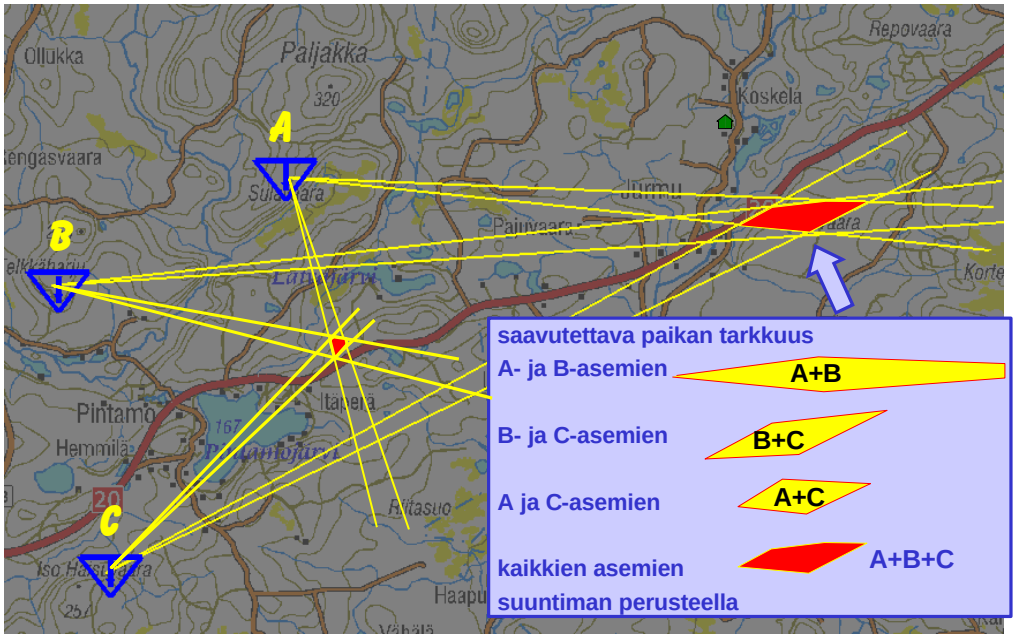



**Kuva 11: Radiohorisontti määrittää käytännössä elektronisen tiedustelun suurimman mahdollisen kantaman. Todellinen kantama riippuu lähettimen ja tiedusteluvastaanottimen ominaisuuksista, erityisesti lähetystehosta ja taajuusalueesta, sekä maaston muodoista ja on usein teoreettista kantamaa lyhyempi, mutta toisaalta tietyissä tilanteissa voi olla myös sitä pidempi.**

Aktiivisten lähetinten havaitseminen on yleensä mahdollista huomattavasti kauempaa kuin mikä näiden järjestelmien oma kantama on. Siten viesti- ja tutkajärjestelmät ovat periaatteessa havaittavissa näiden järjestelmien omaa kantamaa pidemmiltä etäisyyksiltä, tutkajärjestelmän tapauksessa jopa huomattavasti pidemmältä etäisyydeltä kuin miltä tutka itse kykenee havaitsemaan maalin. Tämä johtuu ensisijaisesti siitä, että elektronisen tuen sensorille signaali tulee suoraan tutkan lähettimeltä, mutta tutka saa oman signaalinsa sen heijastuttua maalista. Tällöin tutkasignaali joutuu kulkemaan tutkan ja vastaanottimen välisen etäisyyden kahteen kertaan, kun taas signaali tutkalta elektronisen tuen vastaanottimelle kulkee tämän matkan vain kerran. Tämän vuoksi moderni ELTU-järjestelmä saa lähes aina varoituksen tutkasta ja kykenee paikantamaan sen ennen kuin tutka kykenee havaitsemaan aluksen tai lentokoneen,

joka on varustettu ELTU-sensorilla[i]. Elektronisen tuen kantaman tärkein rajoittava tekijä on maan kaarevuudesta johtuva radiohorisontti. Radioaallon kaartumisen vuoksi radiohorisontti on jonkin verran kauempana kuin näkyvä horisontti. Radiohorisontin sisäpuolella tarkkailtavista kohteista saadaan hyvä signaali, mutta horisontin takana olevista kohteista lähtevä signaali vaimenee nopeasti eikä tiedustelu sen vuoksi juurikaan ulotu radiohorisonttia pidemmälle. Tosin voimakastehoisia lähettimiä, HF-alueen radioliikennettä ja tutkajärjestelmiä sekä tietyissä oloissa muitakin lähetteitä voidaan havaita ja paikantaa horisontin takaakin.

Elektronisen tuen yksi erityinen ominaisuus on se, että joissakin tilanteissa sillä kyetään tunnistamaan joukko tunnistamalla sen käyttämät välineet niiden lähettämien signaalien perusteella. Lisäksi se kykenee viestiliikennettä ja muita lähetteitä tarkkailemalla arvioimaan vastustajan toimintaa.




**Kuva 12: Mittausgeometria vaikuttaa huomattavasti suuntimalla saavutettavaan paikannustarkkuuteen. Paras tulos saavutetaan toisiinsa nähden mahdollisimman suorakulmaisilla suuntimilla. Oikealla olevan lähettimen paikka on epätarkka pienten suuntimakulmien sekä pitkän etäisyyden vuoksi. Vastaavasti vasemmalla paikannustarkkuus riittää tulenkäyttöön suoraan elektronisen tuen havainnon perusteella.**

Käytettävissä olevista haku- ja kuunteluvastaanottimista sekä kohteena olevista viestijärjestelmistä riippuen voidaan vastustajan viestiliikennettä kuunnella. Perinteisen

[i] Poikkeuksen tästä muodostaa vain niin sanottu LPI-tutka (Low Probability of Intercept), joka on jo lähtökohtaisesti suunniteltu siten, ettei vastustajan ELTU-sensori kykenisi sitä havaitsemaan. Luonnonlakien asettamien rajoitusten vuoksi tällaisen LPI-tutkan kantama on kuitenkin yleensä lyhyt (10-20 km luokkaa).

analogisen radiokaluston sekä salaamattoman digitaalisen radiokaluston kuunteleminen on varsin yksinkertaista, mutta myös salattujen lähetteiden kuunteleminen voi olla mahdollista: yksinkertaisesti salatut tai salausalgoritmin heikkouksia sisältävät lähetteet voidaan kuunnella reaaliajassa ja osa tehokkaasti salatuistakin lähetteistä on mahdollista purkaa jälkikäteen tallenteista. Onkin muistettava, että täysin varmoja salausjärjestelmiä ei ole olemassa: on vain kyse siitä paljonko aikaa ja rahaa ollaan valmiit käyttämään salauksen purkamiseen. Elektronisessa sodankäynnissä toiminta on yleensä lähes reaaliaikaista, joten signaalien informaatiosisällön selvittäminen voi olla toissijaista. Päätöksen tekoon riittää lähes aina se, että kohde paikannetaan ja tunnistetaan, eikä salauksen purkamiseen välttämättä edes ole tarvetta.

Maahan sijoitettu elektronisen tuen sensorijärjestelmä kykenee esimerkiksi muodostamaan reaaliaikaisen maalitilannekuvan 40 km x 40 km alueelta kenttäradio-taajuuksilla ja 100 km x 100 km alueelta HF-taajuuksilla. HF-alueella signaalin etenemisominaisuuksien vuoksi voi syntyä aukko alueille, joilta signaali ei enää etene maanpinta-aaltona, muttei myöskään vielä heijastu ionosfäärin kautta (ns. skip zone).

Elektronisen tuen paikantamistarkkuus riippuu:

- Etäisyydestä: Tarkkuus on yleensä muutamia prosentteja mittausetäisyydestä, mutta heikkenee etäisyyden kasvaessa, sillä etäisyyden aiheuttaman vaimennuksen kasvaessa suuntimoon saapuva signaali on vastaavasti heikompi. Tämän vuoksi suuntimot pyritään sijoittamaan mahdollisimman eteen.
- Suuntimokannasta: Mittausgeometrian kannalta tarkin tulos saavutetaan, kun kahdella tai useammalla suuntimolla saatavat suuntimat ovat mahdollisimman suorassa kulmassa toisiinsa nähden.
- Maaston aiheuttamasta vaimennuksesta, jonka minimoimiseksi suuntimot pyritään sijoittamaan mahdollisimman korkealle.
- Tiedusteluasemassa vallitsevasta kohinatasosta, muiden lähettimien aiheuttamista häiriöistä ja maaston, rakennusten, metalliaitojen ja sähkölinjojen aiheuttamista heijastumista. Näiden minimoimiseksi elektronisen tuen asemat pyritään sijoittamaan riittävän etäälle omista viesti- ja tutka-asemista sekä muista häiriöitä aiheuttavista kohteista.
- Radiolähettimen ja tiedusteluvastaanottimien radioteknisistä ominaisuuksista.
- Operaattoreiden ammattitaidosta.

Sensorin passiivisuuden vuoksi ELTU-asemat kykenevät määrittämään kohteen olemassaolon sekä suunnan, jossa havaittu kohde on, mutta eivät määrittämään havaittujen kohteiden etäisyyttä. Tämän vuoksi yksittäinen asema ei kykene paikantamaan kohteita maastoon. Paikantamisen toteuttamiseksi asemien tekemien havaintojen parametri- ja suuntatiedot yhdistetään, ja näin kohde saadaan paikannettua ristisuuntimalla.

**Kuva 13: Vasemmalla elektronisen tuen asema, jolla havaitaan ja seurataan passiivisesti ilma-aluksia. Kuvassa näkyvät eri antennit on tarkoitettu eri taajuus-alueille. Antennit on asennettu tasolle, jota käännetään eri suunnissa olevien maalien etsimiseksi ja seuraamiseksi. Oikealla erikoisjoukkojen käyttöön tarkoitettu kannettava tutkavaroitin. Laitteessa on pyöreiden sääsuojien takana antennit, jotka suunnataan kohti oletettua uhkasuuntaa. Laite mahdollistaa toiminnan maastonvalvontatutkan valvomalla alueella.** [J. Kosola]

## Elektroninen maalinosoitus

Elektroninen maalinosoitus on reaaliaikaista maalien etsintää, paikantamista ja tunnistamista, jonka tavoitteena on asejärjestelmän tarvitseman maalitiedon tuottaminen. Vastustaja ei kykene havaitsemaan passiivista maalinosoitusjärjestelmää, joten se ei saa maalinseurannasta ennakkovaroitusta eikä voi myöskään hyökätä sitä vastaan esimerkiksi tutkasäteilyyn hakeutuvin ohjuksin. Passiivista maalinosoitusta hyödyntävää ilmatorjuntajärjestelmää ei voida myöskään kiertää yhtä yksinkertaisesti kuin aktiivisesti lähettävää ja siten havaittavissa olevaa tutkajärjestelmää. Elektronisen maalinosoituksen tarkkuus riittää tyypillisesti suoraan asejärjestelmän ohjaamiseen lähietäisyydelle sekä tiedustelun ja valvonnan fokusoimiseen maalialueelle pidemmillä etäisyyksillä.

Verkottuneella taistelukentällä, jolla valvonta- ja asejärjestelmien suuri ulottuvuus mahdollistaa nopean ja tarkan tulenkäytön, on merkittäväksi ongelmaksi noussut havaittujen maalien tunnistaminen. Maalipisteet on ensinnäkin kyettävä päättelemään vihollisiksi ja toiseksi on kyettävä päättämään, mitkä lukuisista havaituista maaleista ovat tulenkäytön arvoisia ja mihin maaleihin vaikuttamiseen käytössä olevat voiman-käytön oikeudet riittävät. Elektronisen tuen yksi erityisominaisuus on se, että se (toisin

kuin tutka tai lämpökamera) kykenee useissa tilanteissa tunnistamaan joukon pitkiltä etäisyyksiltä tunnistamalla sen käyttämät välineet niiden lähettämien signaalien perusteella. Elektroninen tuki onkin tulevaisuudessa keskeisimpiä maalintunnistuksen (combat-ID, non-co-operative target recognition) menetelmiä. Tämän kykynsä vuoksi se on jo tällä hetkellä kriisinhallintaoperaatioiden tärkein sensori.

| Elektronisen tuen ominaisuuksia muihin sensoreihin verrattuna | |
|---|---|
| **1. Passiivisuus** | |
| Edut | Sensoria ja joukkoa ei voida havaita vastustajan elektronisen sodankäynnin sensoreilla eikä tuhota lähettimen säteilyyn hakeutuvilla ohjuksilla, joten joukko on paremmin suojassa kuin esimerkiksi tutkajärjestelmä. |
| | Maali ei havaitse, että sitä seurataan eikä siten kykene käynnistämään vastatoimenpiteitä. |
| Heikkoudet | Kohteessa on oltava aktiivinen lähetin: Jos kohde ei lähetä, sitä ei havaita. Tämän puutteen vuoksi ES-järjestelmät eivät korvaa tutkaa, mutta täydentävät sitä erittäin tehokkaasti. On myös muistettava, ettei vastustaja voi aina toimia radiohiljaisuudessa, varsinkaan taistelukosketuksen jälkeen. |
| **2. Maalintunnistuskyky** | |
| Edut | Elektroninen tuki kykenee keräämään tietoja joukkojen käytöstä, painopisteestä, sivusta- ja selustauhkista yms. taisteluun ja komentajan päätöksiin vaikuttavista seikoista. |
| | Elektroninen tuki kykenee seuraamaan joukkoa ja sen toimintaa pitkään sekä sitomaan sen kokonaistilanteeseen, joten ammattitaitoisen elektronisen tuen harhauttaminen on vaikeata eikä onnistu pelkin teknisin keinoin. |
| | Joukkojen tunnistaminen niiden käyttämän radio-, tutka- yms. kaluston sekä viestiliikenteen yms. avulla mahdollistaa omien ja vastustajan joukkojen erottamisen. Tämä mahdollistaa nopean tulenkäytön myös sellaisia maaleja vastaan, joita ei voida visuaalisesti tunnistaa. |
| | Maalien tunnistaminen tukee oman tulenkäytön maalien valintaa ja priorisointia. |
| **3. Reaaliaikaisuus** | |
| Edut | Tilannekuva muodostuu muutamassa minuutissa, uhkavaroitus voidaan antaa sekunneissa. Kykenee maalinseurantaan ja maalinosoitukseen muille sensoreille tai asejärjestelmille, esimerkiksi tykistölle ja ilmatorjunnalle. |

**Taulukko 1: Elektronisen tuen ominaisuuksia muihin sensoreihin verrattuna**

Elektronisen tuen paikannustarkkuus riittää tyypillisesti epäsuoran tulen ohjaamiseen alle 10 km etäisyydellä käytettäessä konventionaalisia (ohjaamattomia) kranaatteja ja 10-40 km etäisyydellä käytettäessä hakeutuvia ammuksia tai suunnattaessa kohdealueelle muuta tiedustelu-, valvonta- ja maalinosoituskykyä, kuten tiedustelu- ja tulenjohtolennokki, tiedustelutulenjohtopartio tai käytettäessä sellaista pitkän kantaman asetta, jossa on itsessään tiedustelukykyä[26].

### Elektroninen uhkavaroitus

Elektroninen uhkavaroitus (Threat Warning) tarkoittaa järjestelmiä, joiden avulla voidaan havaita, paikantaa ja tunnistaa omiin järjestelmiin välittömästi kohdistuva tiedustelu, häirintä ja asevaikutusuhka ja joiden antamien tietojen perusteella voidaan optimoida omat vastatoimet. Uhkavaroitusta voidaan käyttää sekä suojautumis- ja väistötoimenpiteiden käynnistämiseen ja ohjeistamiseen, että omasuoja- ja asejärjestelmän aktivoimiseen ja ohjaamiseen[27]. Elektroninen uhkavaroitus voidaan saada joukkoa tukevalta elektronisen tuen sensorilta tai kohteen omasuojajärjestelmältä. Elektronisen tuen yksikkö kykenee antamaan riittävän ennakkovaroituksen yhtymälle tai useammillekin yhtymille lentorynnäköltä suojautumiseksi ja ilmatorjunnan tulenkäytön ohjaamiseksi.

Omasuojajärjestelmässä olevilta varoittimilta saadaan riittävä ennakkovaroitus omasuojajärjestelmän vastatoimenpiteiden käynnistämiseksi sekä osuman väistämisessä tarvittavien ohjausliikkeiden suorittamiseksi. Erikoisjoukkojen käyttöön on kehitetty keveitä kannettavia ELTU-laitteita, jotka havaitsevat maastonvalvontatutkat ja mahdollistavat partion pysähtymisen ennen kuin tutka havaitsee sen liikkeen. Näin partio voi liikkua maastonvalvontatutkan valvomalla alueella tulematta havaituksi. Tällaisia järjestelmiä kehitetään erikoisjoukkojen käyttöön myös vastustajan johtamispaikkojen, radiolla varustettujen vartiomiesten yms. kohteiden havaitsemiseksi ja paikantamiseksi niiden välttämistä tai tuhoamista varten[28].

## Elektroninen vaikuttaminen

Elektroninen vaikuttaminen (ELVA, engl. Electronic Attack, EA) tarkoittaa hyökkäyksellisiä toimenpiteitä, joilla heikennetään vastustajan toimintakykyä vaikuttamalla sen elektronisiin järjestelmiin. Elektronisen vaikuttamisella pyritään estämään, hidastamaan tai vähentämään vastustajan sähkömagneettista säteilyä hyödyntävien tai elektroniikasta riippuvien järjestelmien käyttöä. Elektronisella vaikuttamisella voidaan myös pyrkiä ohjaamaan vastustajan spektrin käyttöä. Esimerkiksi amerikkalaiset sovelsivat Persianlahden sodassa vuonna 2003 ”tiedonsiirtoyhteyksien paimentamista”, jossa ensin lamautettiin irakilaisten valokuituverkko, mikä pakotti heidät siirtymään radioyhteyksien käyttöön. Sen jälkeen elektronisella häirinnällä ohjattiin irakilaiset käyttämään vain muutamia häiritsemättömiä taajuuksia, joita sitten kyettiin helpommin hyödyntämään tiedustelussa ja jotka oli tarvittaessa suhteellisen yksinkertaista lamauttaa elektronisella häirinnällä[29]. Elektroninen

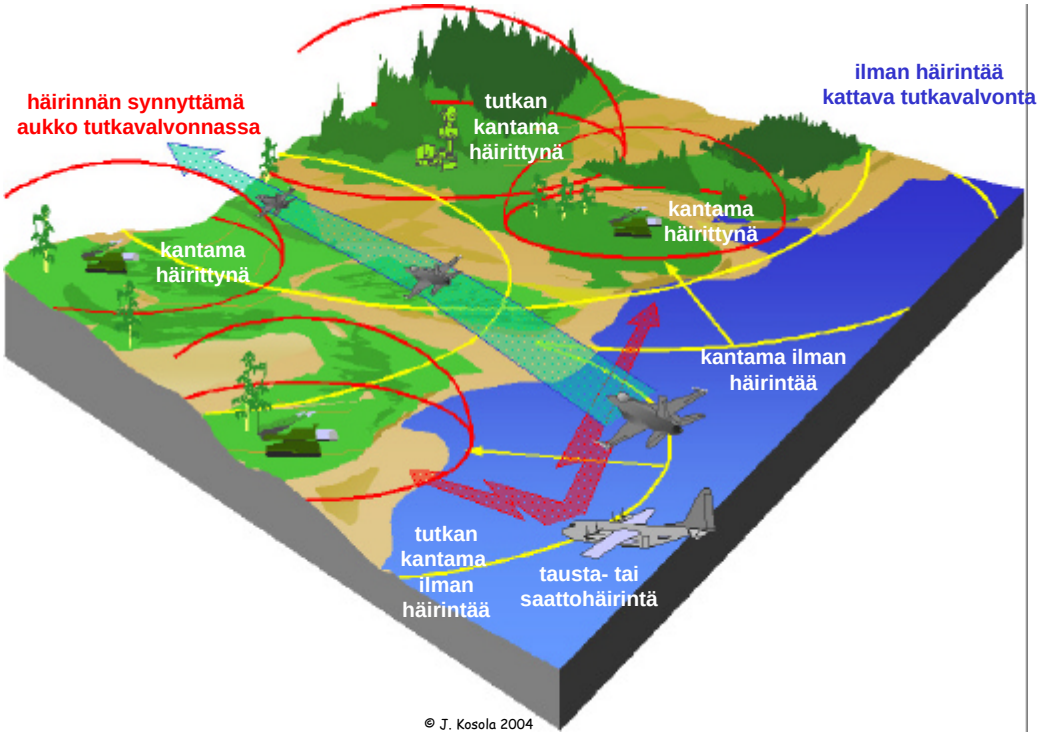
vaikuttaminen jakautuu elektroniseen häirintään, elektroniseen lamauttamiseen, elektroniseen tuhoamiseen ja elektroniseen harhauttamiseen.

**Kuva 14: Norjan armeijan käyttämä HF/VHF/UHF-häirintäjärjestelmä Tor on asennettu Suomessa valmistettuun raskaaseen P6-telakuorma-autoon. Järjestelmässä on häirittäviä järjestelmiä kohti suunnattavat laajakaistaiset kolmiomaiset ns. logaritmisperiodiset antennit eri taajuusalueille. Nostamalla antennit mastoon voidaan häirintäetäisyyttä kasvattaa, mutta tämä rajoittaa häirintää liikkeestä.** [ewation GmbH/MRCM]

## Elektroninen häirintä

Elektronisella häirinnällä (electronic jamming) vaikeutetaan tai estetään vastustajan kykyä hyödyntää sähkömagneettista spektriä. Elektroninen häirintä kohdistuu aina järjestelmien vastaanottimiin. Häirintä voi olla luonteeltaan estävää (peittävää) tai harhauttavaa. Estävällä häirinnällä pyritään vaikeuttamaan vastapuolen kykyä vastaanottaa tietoa sähkömagneettisesta spektristä. Käytännössä tämä näkyy häirittävän järjestelmän maksimitoimintaetäisyyden supistumisena. Esimerkiksi tutkajärjestelmän kantama ja viestijärjestelmällä saavutettavissa oleva yhteysväli supistuvat normaalista

murto-osaan. Ilmapuolustuksen valvonta- ja seurantatutkien häirinnällä pyritään pienentämään valvonta- ja asejärjestelmien tehollista kantamaa niin paljon, että niitä vastaan voidaan hyökätä tutkan supistetun kantaman ulkopuolelta, mutta oman asejärjestelmän kantaman sallimalta etäisyydeltä. Joissakin tilanteissa häirintä on riittävän tehokasta, jos sensori- ja asejärjestelmien kantamaa kyetään pienentämään niin paljon, että vastustajan puolustusjärjestelmään muodostuu aukko, jota vastustaja ei kykene valvomaan tai johon se ei kykene ampumaan ilmatorjuntaohjuksia.

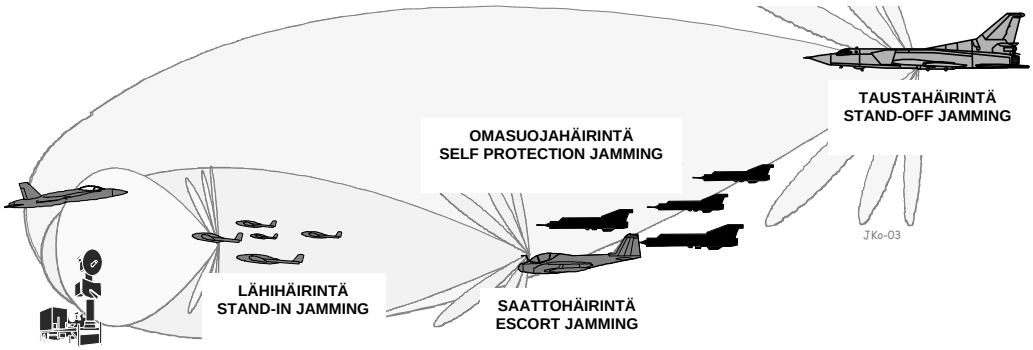



**Kuva 15: Elektroninen häirintä pienentää valvonta- ja asejärjestelmien tutkien kantamaa. Tällöin yhtenäiseen peittoalueeseen muodostuu aukkoja, joita häiritsijä pyrkii hyödyntämään omissa operaatioissaan.**

Johtamisjärjestelmän häirinnällä pyritään katkaisemaan vastustajan johtamisyhteydet ja siten hidastamaan sen toimintaa. Harhauttavalla häirinnällä pyritään vaikuttamaan vastustajaan niin, että se tekisi vastaanottamansa sähkömagneettisen säteilyn perusteella vääriä johtopäätöksiä joukkojen ja laitteiden sijainnista, liikeradasta yms. seikoista.

Häirintä voidaan jakaa myös tuki- ja omasuojahäirintään sen mukaan missä häirintäjärjestelmä on suhteessa häirinnällä suojattavaan kohteeseen. Tukihäirinnässä (support jamming) häirintäjärjestelmä suojaa jotakin muuta järjestelmää – yleensä asejärjestelmää. Tukihäirintä voidaan jakaa edelleen tausta-, saatto- ja lähihäirintään sen mukaan miten häirintäjärjestelmä sijoittuu häirittävään kohteeseen ja häirinnällä suojattavaan kohteeseen nähden.

Taustahäirintä (stand-off jamming) tarkoittaa operaatioalueella toimivaa häirintää, jolla tuetaan operaation suorittamista yleensä omien joukkojen selustassa tai omassa hallussa olevassa ilmatilassa. Pitkän häirintäetäisyyden vuoksi tukihäirinnässä joudutaan käyttämään suuritehoisia häirintälähettimiä ja siten suurikokoisia häirintäjärjestelmiä. Taustahäirintä toteutetaan yleensä ilmasta, jolloin häirintäsignaalin vaimennus on pieni ja häirinnän kantama siten pitkä. Taustahäirinnän tavoitteena voi olla vastustajan sensoreiden häirintä siten, ettei se kykene havaitsemaan operaatioalueella toimivia joukkoja ja järjestelmiä, eikä operaation aikautusta tai suuntautumista. Saattohäirintää (escort jamming) suorittava ajoneuvo, lentokone tai alus liikkuu hyökkäävän osaston mukana ja suojaa sitä vastustajan asevaikutukselta häiritsemällä sen ilmapuolustusjärjestelmän sensoreita. Saattohäirintä paljastaa saatettavan joukon, mutta estää vastustajaa käyttämästä aseita sitä vastaan häiritsemällä maalinosoitus- ja maalinseurantajärjestelmiä. Saattohäirintää suorittavan lavetin – siis ajoneuvon, ilma- tai merialuksen – tulisi kyetä liikkumaan suhteellisen vapaasti hyökkäävän osaston mukana, jotta häirintäsuojaus kyettäisiin toteuttamaan optimaalisesti. Tämä asettaa vaatimuksia sekä häirintälavetin liikehtimiskyvylle, että liikkumismahdollisuuksille taktisessa tilanteessa. Tämä on usein ollut operaatioissa ongelmana.




**Kuva 16: Esimerkki hyökkäysoperaation tukemisesta taustahäirinnällä sekä rynnäkköosaston saatto- ja omasuojahäirinnällä. Ilmapuolustuksen lamauttamisen osana voidaan lisäksi käyttää ohjuksilla, lennokeilla tai erikoisjoukoilla toiminta-alueelle toimitettavia lähihäirintälähettimiä.**

[Kuva teoksesta Digitaalinen Taistelukenttä]

Lähihäirinnässä (stand-in jamming) häirintälähetin viedään hyvin lähelle häirittävää kohdetta. Lyhyt häirintäetäisyys mahdollistaa tehokkaan häirinnän hyvinkin pienillä häirintätehoilla. Pienitehoinen häirintälähetin voidaan rakentaa pienikokoiseksi, keveäksi ja suhteellisen halvaksi. Pieni koko ja kevyt toteutus mahdollistavat häirintälähettimen toimittamisen kohdealueelle monilla erilaisilla menetelmillä, kuten tykistön ja raketinheitinten kantoammuksilla tai sirotteilla. Lähihäirintälähetin voi olla myös lennokkiin tai jopa ilmapalloihin asennettu.

Hyökkäysoperaatioihin liittyvän häirinnän tehoa voidaan lisätä käyttämällä laveteissa häivetekniikkaa. Vaikka elektroninen häirintä tai häivetekniset ratkaisut eivät

kumpikaan yksinään riittäisi aukkojen luomiseen puolustuksen sensoriverkkoon, yhdessä nämä usein mahdollistavat turvallisen hyökkäyskäytävän muodostamisen.

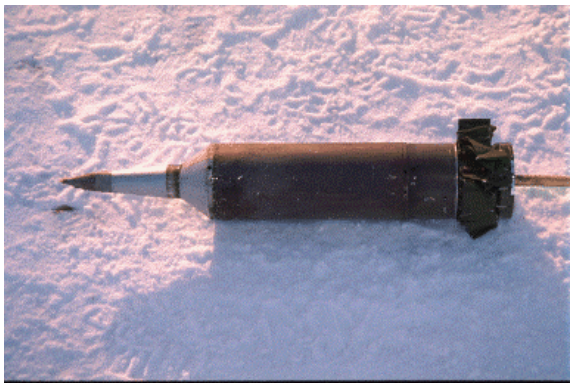
**Kuva 17: Viestitiedustelu- ja häirintäaseman operaattorin työpiste. Varsinaiset ELSO-laitteet on tässä järjestelmässä sijoitettu toisaalle, ja kuvan operaattorilla on käytössään työasemissa järjestelmien ohjelmiston käyttöliittymät.** [ELTA]

Joissakin lähteissä yhtenä elektronisen häirinnän lajina mainitaan myös *passiivinen häirintä*, jolla tarkoitetaan elektroniseen suojautumiseen kuuluvien passiivisten heitteiden, kuten tutkalta suojautumiseksi käytettävän metalloidun silpun levittämistä, tutkasäteilyä absorboivien materiaalien käyttämistä tai infrapunahakuisten ohjusten harhauttamiseksi pudotettavien aktiivisten lämpösoihtujen käyttöä. Nykyisissä määritelmissä nämä kuuluvat yleensä joukon tai lavetin omasuojaan, mutta esimerkiksi silppua voidaan käyttää myös massiivisesti esimerkiksi laajojen joukkosiirtojen peittämiseen.

### Elektroninen harhauttaminen

Elektroninen harhauttaminen (electronic deception) tarkoittaa aktiivisia hyökkäyksellisiä toimenpiteitä, joilla pyritään syöttämään vastustajalle vääriä tietoja omien järjestelmiemme ja joukkojemme määrästä, sijainnista, liikkeestä, aikeista ja teknisistä ominaisuuksista. Elektronisella harhauttamisella vaikeutetaan ennen kaikkea vastustajan valvonta- ja tiedustelutoimintaa, mutta sillä voidaan pyrkiä myös vaikuttamaan vastustajan johtamistoimintaan lähettämällä harhauttavia sanomia ja käskyjä vastustajan komentoverkkoon. Harhauttamiseen voidaan käyttää esim. aktiivisia ja passiivisia tutkavalemaaleja, aktiivisia valelähettimiä sekä

häirintälähettimiä, joiden lähettämien signaalien avulla luodaan valemaaleja vastaanottavaan tutkaan.



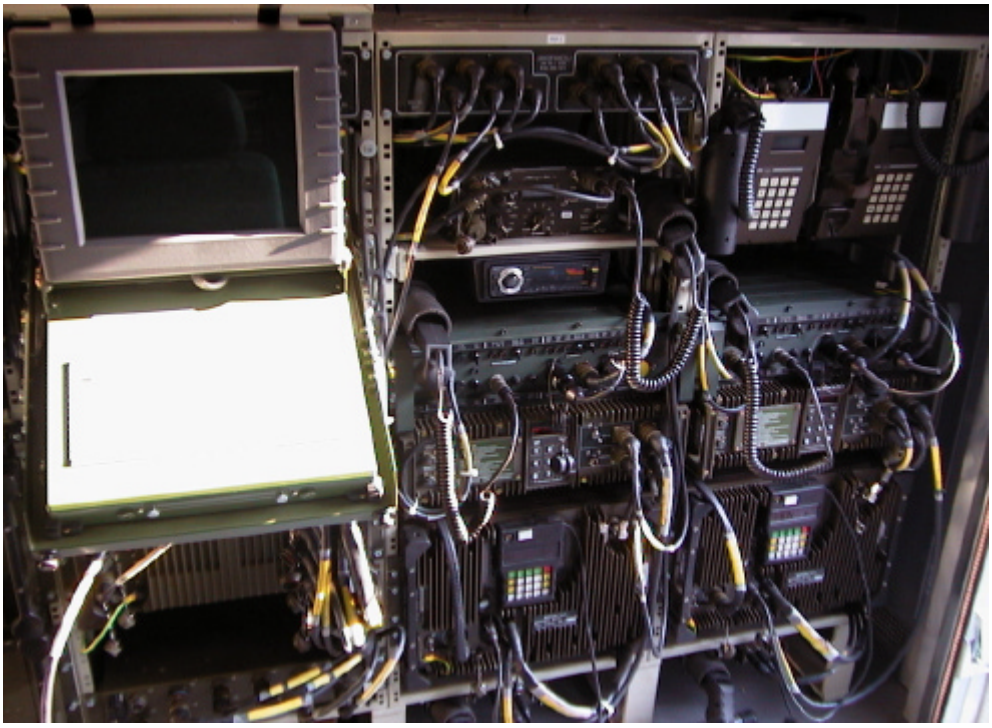
**Kuva 18: Tykistön kantoammuksella maalialueelle toimitettava lähihäirintälähetin on tehokas komentopaikkojen ja viestikeskusten tilapäiseen lamauttamiseen. Häirintälähetin iskeytyy maahan kärki edellä ja nostaa perässä olevan häirintäantenninsa pystyyn.** [SA-kuva]

## Elektroninen lamauttaminen ja tuhoaminen

Elektroninen lamauttaminen tarkoittaa vastustajan elektronisten laitteiden toimintakyvyn heikentämistä niihin kohdistetun sähkömagneettista energian avulla. Lamauttaminen on luonteeltaan tilapäistä, eikä se aiheuta suoraan vastustajan järjestelmään pysyviä vaurioita. Välillisesti pysyviä vaurioita voi syntyä esimerkiksi silloin, kun sensori- tai ohjausjärjestelmän lamauttaminen johtaa ajoneuvon törmäykseen tai ohjuksen maahan syöksymiseen. Elektronisen häirinnän ja lamauttamisen erona on karkeasti se, että edellinen kohdistuu vastaanottimiin ja sillä pyritään estämään vastustajan kykyä vastaanottaa tietoa sähkömagneettisesta spektristä, kun taas lamauttamisella pyritään vaikuttamaan itse laitteen sisäiseen toimintakykyyn. Lamauttaminen voi kohdistua myös järjestelmien lähettimiin. Se toteutetaan samoilla elektronisilla asejärjestelmillä kuin tuhoaminenkin.

Elektronisella tuhoamisella pyritään aiheuttamaan vastustajan elektronisiin laitteisiin pysyviä vaurioita kohdentamalla niihin niin suuri sähkömagneettinen energia, että laitteiden elektroniset komponentit vaurioituvat. Elektronisessa tuhoamisessa voidaan käyttää esimerkiksi *sähkömagneettista pulssia* (EMP, Electromagnetic Pulse) tai *suurtehomikroaaltopulssia* (HPM, High-Power Microwave). Radiotaajuuksilla ja laseraallonpituuksilla toimivista aseista sekä hiukkasaseista käytetään myös yhteisnimitystä *suunnatun energian ase* (DEW, Directed-Energy Weapon).

Suunnatun radiotaajuisen energian aseet voivat tuoda mukanaan vallankumouksellisen mahdollisuuden lamauttaa vastustajan elektroniset järjestelmät ja niiden operatiivista käyttöä pidetään todennäköisenä tulevaisuudessa[30]. Näiden aseiden erittäin voimakastehoiset radiotaajuiset signaalit kykenevät häiritsemään elektronisesti ohjattuja järjestelmiä johtamisjärjestelmien tietokoneista ohjusten hakupäihin. Suunnatun energian aseista erityisesti suurtehomikroaaltoase, eli HPM-ase, on muodostumassa todellisuudeksi taistelukentällä. Tämän epäkonventionaalisen aseen perusluonne, näkymätön ja monesti jopa täysin huomaamaton vaikuttaminen, tuo mukanaan monipuolisia vaikutusmahdollisuuksia. Kohteita voidaan esimerkiksi lamauttaa niiden sitä itse havaitsematta. Aseen käyttökynnystä madaltaa lisäksi se, ettei sillä ole vaikutusta muihin kuin elektronisiin laitteisiin, joten oheisvahinkojen pelko ei rajoita aseen käyttöä kriisitilanteissa. Erityisen sovelias se on lyhyen kantaman sovelluksiin, kuten erittäin lyhyen kantaman ohjus- ja ilmatorjuntajärjestelmiin sekä kohteen välittömään läheisyyteen toimitettavien täsmäaseiden taistelukärkiin tai erikoisjoukkojen käyttöön. Radiotaajuisia aseita käsitellään laajemmin liitteessä 4.



**Kuva 19: Sodankäynnin riippuvuus elektroniikasta on niin keskeinen, että elektroniikan käytön kyseenalaistavat vaikuttamisjärjestelmät sekä näiltä suojautuminen ovat puolustusjärjestelmän toiminnan kannalta kriittinen alue. Kuvassa suomalaisen prikaatin ja armeijakunnan viestijärjestelmän YVI2-viestiaseman tiedonkäsittely- ja tiedonsiirtolaitteita.** [J. Kosola]

Laserilla kyetään vaurioittamaan elektro-optisten eli optronisten järjestelmien herkkiä ilmaisimia ja joissakin tapauksissa myös optiikkaa sekä järjestelmäoptiikan käyttämiä suojaikkunoita. Erittäin suuritehoisilla lasereilla voidaan tuhota jopa ballistisia ohjuksia

ja tykistöraketteja, mutta tällaiset järjestelmät ovat ainakin vielä niin suurikokoisia, että niiden käyttö rajoittuu strategisten kohteiden suojaamiseen. Sen sijaan pelkkään optisten tähystysvälineiden tilapäiseen tai pysyvään sokaisuun tarkoitettujen järjestelmien vaatima teknologia on olemassa jo nykyisin. Esimerkiksi taistelu-helikopterin pimeänäkölaitteen sokaisemiseen vaaditaan vain muutaman watin laserteho. Laseria käytetäänkin erityisesti elektronisen suojautumisen yhtenä toteuttamistapana. On kuitenkin huomattava, että hyökkäykselliseen operaatioon liittyen on teknisesti mahdollista lamauttaa tai häiritä paitsi vastustajan radiotaajuiset sensorit, myös sen optroniset järjestelmät.

**Kuva 20: Amerikkalaisen EA-6B Prowler –koneen häirintälähettimistä osa on sijoitettu siipiripustimiin asennettuihin säiliöihin. Koneen tehtävänä on rynnäkkökoneiden saatto- ja tukihäirintä sekä ilmapuolustuksen lamauttaminen (SEAD), jota varten se voidaan varustaa myös tutkaan hakeutuvilla HARM-ohjuksilla. Häirintäsäiliöissä on radioaaltoja läpäisevästä materiaalista tehtyjä ”ikkunoita” vastaanotto- ja lähetysantennien kohdalla. Pienten lentokoneiden sähköntuotantoteho ei riitä suuritehoiseen häirintään, minkä vuoksi häirintä-säiliöissä voi olla oma potkurilla toimiva sähkögeneraattori.** [S. Heiskanen]

Amerikkalaisessa käsitemaailmassa elektroninen sodankäynti määritellään toiminnan tavoitteen – ei siis toimintamedian, kuten Suomessa – perusteella. Siten amerikkalaiset lukevat myös vastustajan elektronisten laitteiden tuhoamisen ohjuksin osaksi elektronista sodankäyntiä, kun Suomessa tämä olisi osa normaalia fyysistä ase-vaikutusta. Siten tutkasäteilyyn hakeutuvat ohjukset (ARM – Anti-Radiation Missile) osana vastustajan ilmapuolustuksen lamauttamista (SEAD – Suppression of Enemy Air Defenses) tai konventionaaliset ohjukset osana sen tuhoamista (DEAD – Destruction of Enemy Air Defenses) ovat osa USA:n elektronista sodankäyntiä. Tämän *hard* ja *soft*

*kill*:iä yhdistävän toimintamallin ymmärtäminen on keskeistä. Vastustajan elektronisen sodankäynnin järjestelmät ja joukot sekä sensori- ja johtamisjärjestelmät ovat vastustajan suorituskyvyn kannalta niin keskeisiä, että niiden häiritseminen, lamauttaminen tai tuhoaminen tulee nähdä kaikkien asejärjestelmien keskeisenä tehtävänä.

## Elektroninen suojautuminen

Elektroninen suojautuminen (ELSU, engl. Electronic Protection, EP) tarkoittaa toimenpiteitä, joilla pyritään takaamaan omien elektronisten järjestelmien toimintakyky ja joilla vaikeutetaan vastustajan tiedustelutoimintaa. Elektroninen suojautuminen on luonteeltaan puolustuksellista, vaikka jotkut sen menetelmistä perustuvatkin aktiiviseen vaikuttamiseen. Puolustusvoimien määritelmän mukaan elektroninen suojautuminen jaetaan aktiiviseen ja passiiviseen suojautumiseen. Määritelmä on teknislähtöinen. Operatiivisen tarkastelunäkökulman kannalta on parempi jakaa suojautuminen seuraavasti:

1. suojautuminen elektroniselta tiedustelulta ja sen tukemalta asevaikutukselta
2. suojautuminen elektroniselta vaikuttamiselta
3. suojautuminen asejärjestelmiltä

Elektronista suojautumista tarkastellaan seuraavaksi edellä kuvatun operatiivisen tarkastelunäkökulman mukaisesti.

### Suojautuminen elektroniselta tiedustelulta ja sen tukemalta asevaikutukselta

Suojautuminen elektroniselta tiedustelulta ja sen tukemalta asevaikutukselta tarkoittaa sitä, että taistelukentän järjestelmät suunnitellaan ja niitä käytetään siten, etteivät ne paljastu vastustajan elektroniselle tiedustelulle ja altistu sen tukemalle asevaikutukselle. Käytännössä ei ole mahdollista estää järjestelmiä paljastumasta, mutta ne voidaan kuitenkin suunnitella siten, että teknisin keinoin ja oikealla järjestelmien käytöllä voidaan toimia myös vastustajan suorittaman elektronisen tiedustelutoiminnan aikana. Tämä edellyttää kuitenkin järjestelmien suunnittelemista jo alun perin toimimaan elektronisessa uhkaympäristössä. Tällöin on kyettävä sovittamaan yhteen vastustajan aiheuttama uhka sekä oman järjestelmän tekniset ominaisuudet ja järjestelmän käyttöperiaatteet. Järjestelmien kehittäminen ja hankinta on siten tehtävä kokonaisuutena, jossa samanaikaisesti tarkastellaan uhka-arviota, operatiivista konseptia ja järjestelmän teknisiä vaatimuksia. Sotavarustuksen hankintaa käsitellään myöhemmin luvussa *Elektronisen sodankäynnin huomioiminen kehittämisohjelmissa*. Teknisiä keinoja sotavarustuksen toimintaedellytysten takaamiseksi käsitellään kirjassa *Digitaalinen taistelukenttä – informaatioajan sotakoneen tekniikka*.

Suojautuminen vastustajan elektroniselta tiedustelulta kulminoituu emissioiden eli omien lähetteiden, hallintaan ja sitä tukevaan taajuushallintaan. Emissioiden hallinnalla (EMCON, Emission Control) tarkoitetaan omien järjestelmien toiminnallisten ja tahattomien sähkömagneettisten emissioiden[31] tuntemista ja minimoimista siten, että minimoidaan vastustajan mahdollisuudet havaita, analysoida, luokitella, tunnistaa, yksilöidä ja paikantaa järjestelmiämme sekä estetään järjestelmiämme vastaan kohdistuvien vastatoimien optimoimista. Emissioiden hallinnan tulee olla kokonaisvaltaista: esimerkiksi taistelualuksen keittiön mikroaaltouunin vuotosäteily voidaan havaita tiedustelujärjestelmällä yllättävän kaukaa, päälle unohtuneista matkapuhelimista puhumattakaan. Lisäksi emissioidenhallinnassa on huomioitava koko spektri: toimintavapaudet ja -rajoitukset on määriteltävä myös elektro-optisille järjestelmille: esimerkiksi missä tilanteessa, millä alueella, mihin suuntaan ja minä kellonaikoina lasermittaus tai maalinvalaisu on sallittu tai kielletty.

Suojautumiseen voidaan käyttää myös välillisiä keinoja, kuten vastustajan tiedustelu- ja valvontajärjestelmän tukkimista suurella informaatiomäärällä ja tilannekuvan muodostamisen hidastamista harhauttamalla.

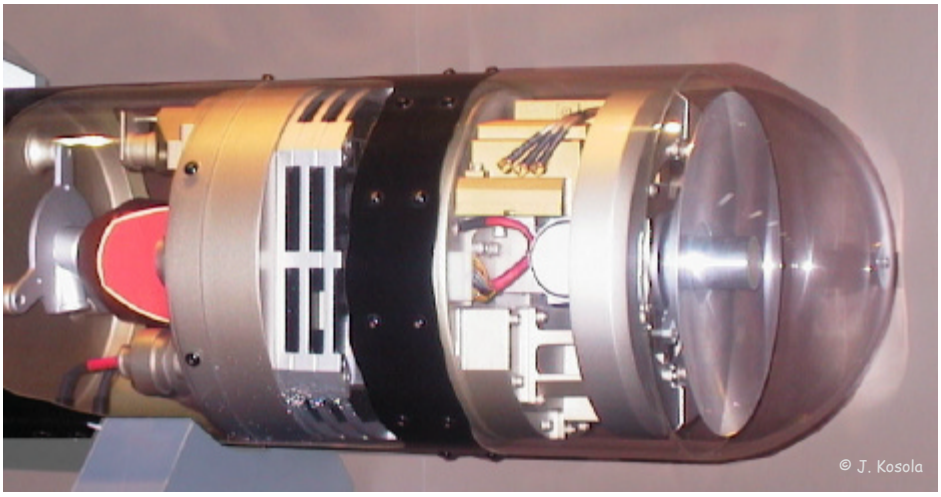
Toiminnallisia keinoja, kuten emissioiden hallintaa, taajuushallintaa ja liikkeen hyödyntämistä käsitellään kirjan toisessa osassa.

### Suojautuminen elektroniselta vaikuttamiselta

Myös vastustaja hyödyntää elektronista vaikuttamista ja käyttää omia järjestelmiämme vastaan tilanteen ja mahdollisuuksiensa mukaan kaikkia edellä kuvattuja elektronisen vaikuttamisen menetelmiä. Tämän vuoksi on tärkeätä suojata omat tiedustelu-, valvonta-, johtamis- ja asejärjestelmät vastustajan elektroniselta sodankäynniltä. Sensori- ja tiedonsiirtojärjestelmien suojaa elektronista häirintää ja harhauttamista vastaan on kehitetty jo toisesta maailmansodasta lähtien. Elektroniikan kasvava käyttö asejärjestelmissä on johtanut siihen, että myös ne ovat tulleet entistä alttiimmiksi elektronisille vastatoimille. Erilaisten omasuojajärjestelmien kehittäminen ja käyttöönotto edellyttävät asejärjestelmien elektronista suojaamista.

Elektroniselta vaikuttamiselta suojautuminen käsittää sekä toiminnallisia että teknisiä keinoja, kuten järjestelmien vahvistamisen kestämään haitallista sähkömagneettista säteilyä (elektroninen vahvistaminen, engl. electronic hardening), järjestelmien oikean käytön ohjeistamista ja suunnittelua, sekä erilaisia mahdollisia toimenpiteitä häirinnän alla. Erilaisia teknisiä häirinnänväistömenetelmiä on hyvin paljon[j], sillä elektronisessa sodankäynnissä on usein kyse jatkuvasta kilpailusta häirintätekniikkaa ja häirinnänväistömenetelmiä kehittävien tahojen välillä. Teknisiä keinoja käsitellään tarkemmin Maanpuolustuskorkeakoulun Tekniikan laitoksen julkaisussa *Digitaalinen Taistelukenttä*. Liitteessä 3 on käsitelty toiminnallisia keinoja vastustajan elektroniselta vaikuttamiselta suojautumiseksi.

[j] Häirinnänväistömenetelmiä kutsuttiin aiemmin englanninkielisessä kirjallisuudessa ECCM-lyhenteellä (Electronic Counter-Counter Measures). Termi ei ole enää virallinen USA:n tai NATO:n käyttämä termi, mutta siitä huolimatta laajassa käytössä etenkin USA:ssa.




**Kuva 21: Älykkyyden lisääntyminen asejärjestelmissä asettaa ne alttiiksi vastustajan omasuojajärjestelmien elektroniselle vaikuttamiselle. Ase-vastatoimi-vastatoimen vastatoimi -ketjussa tekninen kamppailu on jatkuvaa. Kuvassa aktiivisella millimetritutkalla varustettu brittiläinen Brimstone-ohjuksen hakupää, jossa oikealla näkyy tutkan pieni antenni.** [J. Kosola]

## Suojautuminen asejärjestelmiltä

Elektronisen sodankäynnin keinoin voidaan suojautua asejärjestelmiltä estämällä maalin havaitseminen vaikuttamalla tiedustelujärjestelmän tai asejärjestelmän etsintäsensoreihin, estämällä asejärjestelmän maalinseuranta tai lukittuminen maaliin vaikuttamalla maalinosoitus- tai maalinseurantajärjestelmään sekä estämällä aseen osuminen tai suunnitelman mukainen toiminta vaikuttamalla maalinseuranta-järjestelmiin, ammusten komentolinkkeihin, hakupäihin ja herätesytyttimiin. Ase-järjestelmiltä suojautumisessa on kyettävä yhdistämään sekä elektronisen tuen ja elektronisen häirinnän että häivetekniikan menetelmiä optimaalisen kokonaisuuden muodostamiseksi.

Taistelukentän järjestelmien kallistumisen sekä korkeateknologisen uhan kasvun myötä ***omasuojajärjestelmät*** ovat tulossa myös maavoimien keskeisiin lavetteihin. Oma-suojajärjestelmän tavoitteena on varoittaa lavetin henkilöstöä uhkaavista ase-järjestelmistä sekä saada vastustajan asejärjestelmä harhautumaan maalista tai tuhota ase ennen kuin se ehtii vaikuttaa suojattavaan kohteeseen. Omasuojajärjestelmät ovat osa kohteen kokonaissuojaa ja ne liittyvät kiinteästi sekä tilannetietoisuuteen että lavetin herätteen minimointiin. Häivetekniikan avulla saadaan vähennettyä kohteen herätettä, mikä puolestaan lyhentää sensoreiden havaitsemis- ja tunnistamisetäisyyksiä. Näitä voidaan edelleen lyhentää elektronisella häirinnällä. Käyttämällä kohdetta lisäksi siten, etteivät uhkaavat sensorijärjestelmät pääse havaitsemis- tai tunnistamis-etäisyydelle, kohde on suojassa. Mikään edellä mainituista tekijöistä ei kuitenkaan yksinään tuo riittävää suojaa.


**Kuva 22: Elektronisen sodankäynnin keinot vaikuttaa asejärjestelmän toiminta-ketjuun.**

Täsmäaseiden kehittyminen on mahdollistanut pistemaalien systemaattisen tuhoamisen sekä tykistöllä että ilmasta. Aseissa käytettävän teknologian halpeneminen ja sitä seurannut täsmäaseiden yleistyminen puolestaan luovat sodanjohdolle mahdollisuuksia hyökätä täsmäasein yhteiskunnan infrastruktuurin ja strategisten maalien lisäksi myös taktisen tason kohteita vastaan. Vastaavasti puolustajan on toimintakykynsä säilyttääk-seen kehitettävä kykyä suojata elintärkeitä kohteitaan täsmäaseilta.

Suojaamisessa on käytettävä kustannustehokkaassa suhteessa elektronista vaikutta-mista ja suojautumista, häive-, maastouttamis- ja harhautusmenetelmiä. Ilma-aluksissa tämä voi tarkoittaa esimerkiksi tutkavaroittimen ja ohjusvaroittimien käyttöä sekä silpun/soihdunheitintä ja omasuojahäirintälähettimien käyttöä. Tarvittava varoitin- ja vastatoimenpidelaitteistokokonaisuus riippuu lavettiin kohdistuvasta uhkasta.

Lentokoneissa perinteisen tutkavaroittimen, silpun- ja/tai soihdunheittimen sekä tutka-häirintälähettimen muodostaman yhdistelmän lisäksi (passiivinen) ohjusvaroitin-soihdunheitin ja ennen kaikkea ohjusvaroitin-infrapunahäirintälähetin -yhdistelmät, joissa käytetään laserilla toteutettua suunnattua infrapunahäirintää (Directed IR Countermeasures, DIRCM), tulevat yleistymään matalalla toimivissa laveteissa. Niiden yleistymistä lisäävät lisäksi erilaiset sotaa matalammat konfliktit, joissa yhtenä merkittävänä uhkana on koneiden nousu- ja laskuvaiheessa tapahtuva hyökkäys esimerkiksi olkapääohjuksin.


**Kuva 23: Nykysodissa täsmäaseiden rooli on keskeinen: niillä tuhotaan tärkeimmät pistemaalit, kuten komentopaikat, johtamisjärjestelmän asemat, ilmatorjunta-asemat, huoltokeskukset, satamalaitteet, sillat, padot, voimalaitokset sekä hyökkäyksen pysäyttävät pesäkkeet. Vastaavasti kyky suojautua vastustajan täsmäaseilta muodostuu sodankäynnin perusedellytykseksi. Vasemmalla venäläinen laserohjattava Kilotov-kranaatti, oikealla laserohjattavan pommin ohjausyksikkö.** [J. Kosola]

Tutkahäirintälähetin on 1990-luvulla osin siirtynyt lentokoneesta sen perässä vedettäväksi hinatteeksi (towed decoy), johon tutkahakuisen ohjuksen halutaan harhautuvan. Säteenseuraajaohjusten yleistyminen lisää myös laservaroittimien käyttöä lentokoneiden omasuojajärjestelmissä.

Maalaveteissa käytetään uhkasensorina uhkatyypistä riippuen tyypillisesti laser- ja millimetriaaltotutkavaroitinta ja suojaukseen multispektraalisia (visuaali- ja infrapuna- sekä millimetriaaltoalueen) heitteitä ja mahdollisesti infrapunahäirintäjärjestelmiä. Maasovelluksissa omasuojajärjestelmät eivät ole yleistyneet samassa määrin kuin ilmassa ja merellä liikkuvissa aluksissa. Ensisijaisena syynä tähän on omasuoja-järjestelmän suhteessa korkeampi hinta lavetin hintaan nähden sekä monitahoisempi uhkaympäristö, jossa reagointiaikaa on lyhyiden ampumaetäisyyksien vuoksi hyvin vähän. Kustannustehokkain keino maalla on edelleen tutka- ja infrapunaherätteen hallinta rakenne- ja materiaaliteknisin keinoin sekä yksinkertaisten multispektraali-heitteiden käyttö.

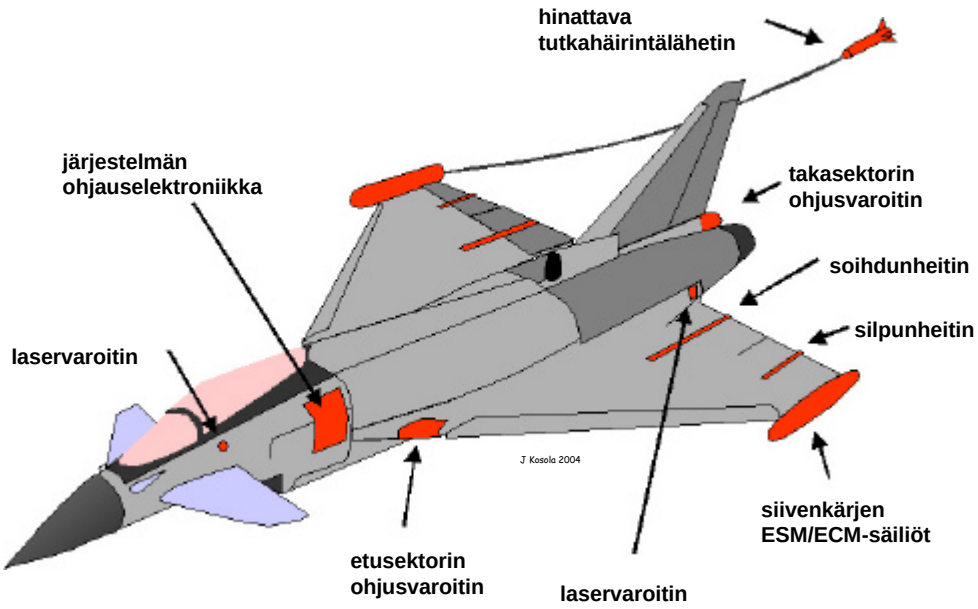
Laivojen omasuojajärjestelmissä käytetään elektronisen tuen passiivista sensoria sekä laservaroitinta ilmaisemaan tulevaa uhkaa ja perinteisiä (infrapuna- ja tutka)heitteiden ja manöövereiden yhdistelmiä suojautumisessa. Miehittämättömien pinnassa liikkuvien alusten ja lennokeiden tai muiden lentävien häirintälavettien käyttö mahdollistaa realistisesti liikkuvan maalin herätteen luomisen riittävän kauas suojattavasta kohteesta ilman heitteiden toiminta-aikarajoituksia. Multispektraalinen sumu voi tekniikan kehittyessä tarjota hyvän suojan täsmäaseita vastaan.

**Kuva 24: Perässä vedettävät valemaalit, *hinatteet,* ovat tehokas tapa suojata lentokoneita ja laivoja. Kuvassa saksalainen Tornado vetää Sky buzzer –tutkaharhamaalia.** [EADS ]

Omasuojajärjestelmien rooli on ollut erilainen eri puolustushaarojen laveteissa. Merivoimien lavetit ovat kalleimpia, eikä niillä ole käytännössä kykyä vetäytyä taistelukosketuksesta niiden tultua kerran havaituksi. Maavoimien lavetit puolestaan ovat edellisiä halvempia ja kykenevät myös hyödyntämään maaston ja kasvillisuuden suojaa. Ilmassa ilman maaston suojaa toimivat ilmavoimien lavetit kykenevät liikehtimään nopeammin. Näiden seikkojen vuoksi puolustushaarojen omasuojajärjestelmäratkaisut poikkeavat toisistaan. Toisaalta maavoimien järjestelmien kallistuminen ja väheneminen sekä omien tappioiden minimoiminen ovat lisäämässä omasuojajärjestelmien käyttöä myös maalaveteissa.

## Sotamoodien käyttö elektronisen suojautumisen turvaamisessa

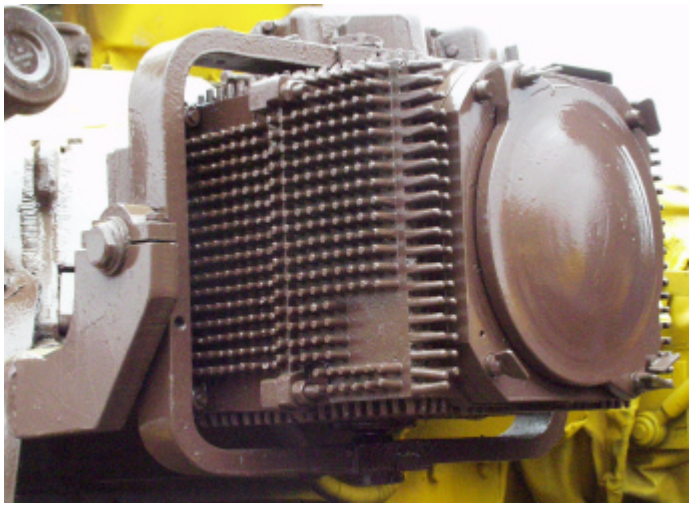
Sotamoodit (wartime reserve modes, WARM) tarkoittavat sensori-, tiedonsiirto-, navigointi-, omatunnistus-, omasuoja-, ase- ja ELSO-järjestelmien teknisiä ominaisuuksia, jotka vaihdetaan sotatilanteessa erotukseksi rauhanaikaisessa harjoituskäytössä olleista ominaisuuksista. Tällä pyritään vaikeuttamaan vastustajan kykyä tiedustella ja häiritä järjestelmiämme sota-aikana vähentämällä vastustajan rauhan aikana suorittaman elektronisen ja muun tiedustelun merkitystä: rauhan aikana järjestelmistä eri menetelmillä kerättävät tiedot eivät enää kriisitilanteessa pidäkään paikkaansa. Sotamoodien käyttöönoton myötä muutettavia parametreja ovat esimerkiksi keskitaajuus, kaistanleveys, lähetysteho, salausalgoritmi ja taajuudenhypytysnopeus.




**Kuva 25: Esimerkki hävittäjäkoneen omasuojajärjestelmästä. Se voi käsittää laservaroittimen lasersäteenseuraajaohjusten havaitsemiseksi, passiivisen IP- tai UV-alueella toimivan ohjusvaroittimen, tutkavaroittimen (ESM), soihtujen ja silpun heittimet ja omasuojahäirintälähettimet (ECM) sekä koneessa että perässä vedettävässä hinatteessa. Kuvassa Eurofighter Typhoon -koneen omasuoja-järjestelmäkokonaisuus. Varoittimien ja häirintäjärjestelmien ilmaisimet ja antennit tulee sijoittaa siten, että kaikki mahdolliset uhkasuunnat tulevat katettua.** [J. Kosola]

Julkisessa materiaalissa sekä asenäyttelyissä esitetään usein laitteille vain suuntaa-antavia suorituskykyominaisuuksia. Kullekin asiakkaalle voidaan kuitenkin räätälöidä ”ylimääräistä” suorituskykyä tämän toiveiden ja maksuhalukkuuden mukaan. Esimerkiksi tutkan hypintäkaistaksi ilmoitetaan julkisesti 300 MHz, mutta asiakkaalle myydään 800 MHz:n hypintäkaista. Tästä asiakas varaa 500 MHz sotamoodeille ja käyttää rauhan aikana harjoitustoiminnassaan vain 300 MHz:n kaistaa. Siirtyminen kriisitilanteessa sotamoodien käyttöön voi yllättää vastustajan tiedustelu- ja valvonta-järjestelmän, joka ei kykene liittämään saamiaan mittaushavaintoja mihinkään aiemmin tuntemaansa järjestelmään. Parhaassa tapauksessa vastustajan häirintäjärjestelmä ei kykene toimimaan koko sotamoodien mahdollistamalla toimintakaistalla.

Varsin usein, ellei peräti lähes poikkeuksetta, valmistajamaan omille asevoimille myydään vientiversioita kehittyneempiä järjestelmiä. Vastaavasti vientiversioista voidaan poistaa joitakin häirinnänväistöominaisuuksia. Asiakkaan on aina kyettävä sekä määrittämään haluamansa elektronisen suojautumisen toiminnalliset ja tekniset vaatimukset, että myös todentamaan niiden täyttyminen vastaanottotarkastuksissa. Tyypillisesti asiakkaalle myydään juuri niin hyvää tai huonoa kun tämä osaa vaatia ja kykenee todentamaan – tai niin hyvää kuin osaa ja haluaa maksaa. Tässä asiassa korostuu oman teknisen henkilöstön osaamistason merkitys: mitä osataan vaatia ja todentaa.



**Kuva 26: Venäläinen Shtora-omasuojahäirintäjärjestelmä on tarkoitettu panssarintorjuntaohjusten maalinseuraimen häirintään. Kuvassa järjestelmän infrapunahäirintälähetinyksikkö, jonka lähettimen ikkunan päällä on kuvassa näkyvä pyöreä suojalevy. Suurin osa lampun tehosta kuluu hukkaan lämpönä, minkä vuoksi järjestelmä tarvitsee yksikön sivulla näkyvät suurikokoiset jäähdytinsäleiköt.** [J. Kosola]

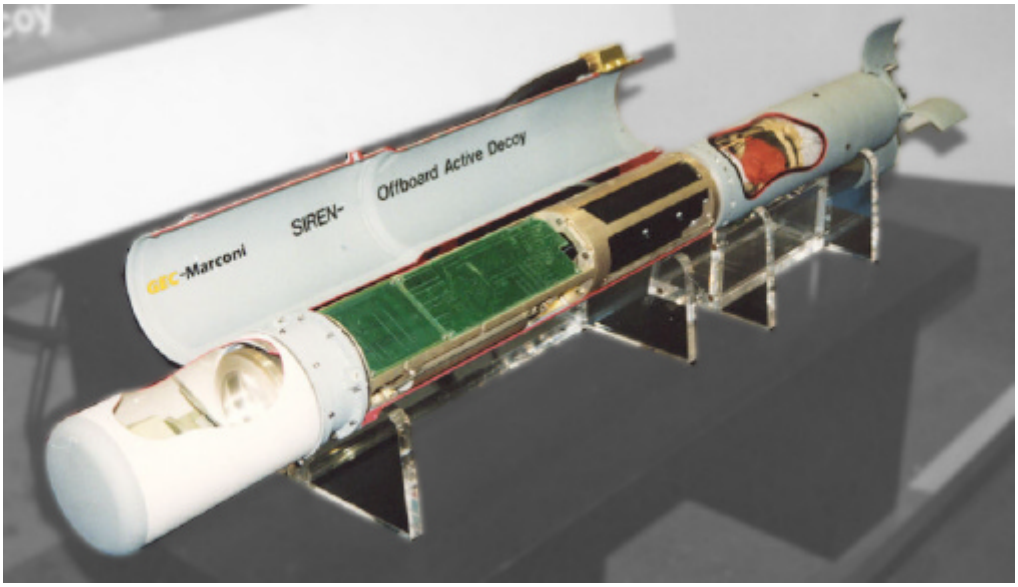
On huomattava, että sotamoodit tuovat suojaa vain mikäli ne pysyvät salaisina. Siten järjestelmien koulutus- ja harjoituskäytön sekä operatiivisen käytön ohjeistaminen tätä taustaa vasten on ehdottoman välttämätöntä. Nämä salassapitonäkökulmat on huomioitava myös järjestelmädokumenttien laadinnassa, jakelussa ja säilytyksessä sekä varastointi-, kuljetus-, huolto- ja logistiikkajärjestelmien toiminnassa ja sen toimitilojen suojaamisessa. Siirtyminen sotamoodien käyttöön on toteutettava vain erikseen käskettäessä, jotta omaa sodan ajan suorituskykyä kyetään takaamaan mahdollisimman pitkälle.

## Elektronisen sodankäynnin tukitoiminta

ELSO-tukitoiminta (Electronic Warfare Support) tarkoittaa niitä toimenpiteitä, joilla luodaan edellytykset järjestelmien toiminnalle elektronisen taistelukentän olosuhteissa tuottamalla elektroniselle tuelle, elektroniselle vaikuttamiselle ja elektroniselle suojautumiselle järjestelmien ohjelmointiin ja käyttöön liittyviä perusteita. ELSO-tuen välittämät tiedot ovat hyvin monitasoisia: ELSO-sensorijärjestelmien parametroinnista (kohteiden tunnistukseen tarvittavat signaalikirjastot) häirintäjärjestelmien tarvitsemiin kohdejärjestelmäspesifisiin häirintämenetelmiin sekä erilaisiin ELSO-toiminnan kehittämisessä tarvittaviin suorituskykyarvioihin. Järjestelmien parametrointi käsittää neljä toimintavaihetta[32]:

1. Tunnistetaan uhkaympäristössä ja uhkajärjestelmissä tapahtunut muutos.
2. Analysoidaan, onko muutoksella vaikutusta omaan järjestelmäämme.

3. Määritetään tarvittavat muutokset tiedustelu-, valvonta-, johtamis-, ase- ja omasuojajärjestelmiin.
4. Tehdään mahdollisesti tarvittavat ohjelmisto- tai tietokantamuutokset, testataan ne ja toimitetaan ne tarvitsijoille.




**Kuva 28: GEC-Marconin aluksen SIREN-omasuojaharhamaali. Laite laukaistaan omalla rakettimoottorillaan ilmaan, missä se laskuvarjon varassa laskeutuessaan voi turvallisesti luoda lähestyvälle meritorjuntaohjukselle suojattavaa alusta houkuttelevamman harhamaalin muutaman minuutin ajaksi.** [S. Heiskanen]

ELSO-tuki on toimintaa, jonka avulla strategisen signaalitiedustelun ja muiden tiedustelulajien tuottamilla tiedoilla tuetaan eri puolustushaarojen operatiivista ELSO-toimintaa. ELSO-tukitoimintaa suorittaa tyypillisesti oma yksikkö (ELSO-tukikeskus; Electronic Warfare [Operational] Support Centre), mutta vastuita voi olla myös jaettu puolustushaaroille. ELSO-tukitoiminta on myös operatiivis-taktista tukea operatiivisen ja taktisen tason elektronisen sodankäynnin joukoille. Tällöin kohdejärjestelmien sijasta toiminta keskittyy kohdeorganisaatioihin ja niiden toimintaan erilaisissa taistelutilanteissa. Nämä tiedot vaikuttavat suoraan ELSO-järjestelmien tuottamiin automaattisiin elektronisiin taistelujaotuksiin (EOB, Electronic Order of Battle), ELSO-joukkojen koulutukseen ja toiminnan suunnitteluun, sekä laajemminkin elektronisen taistelukentän uhkakuvana koko puolustusvoimien operatiiviseen suunnitteluun.

ELSO-tukitoimintaa tarvitaan kaikilla ELSO:n taajuusalueilla, kuten tutka- ja viestijärjestelmien sekä elektro-optisten järjestelmien taajuuksilla. Tukitoiminnan tuottamia tietoja käytetään järjestelmätason lisäksi toimintaa ja taktiikkaa suunniteltaessa ja koulutettaessa. Teknisessä ELSO-tukitoiminnassa käytetään erilaisia laboratoriojärjestelmiä omasuojajärjestelmien ja häirintäjärjestelmien parametroinnin ja häirintämenetelmien kehityksen tukena. On huomattava, että ***ELSO-tukitoiminta*** ei

tarkoita samaa kuin edellä kuvattu ***elektroninen tuki***, vaikka termit muistuttavatkin toisiaan.


**Kuva 27: ELSO-tukitoiminta luo edellytykset elektronisen sodankäynnin kyvylle tuottamalla operaatioiden suunnittelussa sekä ELSO-järjestelmien ohjelmoinnissa tarvittavat tiedot.**

## Puolustushaarakohtaisia vivahteita

Elektronisella sodankäynnillä on kussakin kolmessa puolustushaarassa omat erityispiirteensä. ***Maavoimien*** elektronisen sodankäynnin järjestelmä koostuu yleensä komppanian kokoisista elektronisen tuen osastoista, häirintäosastoista, tykistöllä ammuttavista lähihäirintäkranaateista sekä erikoisjoukkojen käyttämistä kannettavista lähihäirintälähettimistä ja kannettavista hakusuuntimoista. Lisäksi järjestelmään voi kuulua elektronisen tuen tai vaikuttamisen lennokkiyksikkö tai vaihtoehtoisesti joukko voi saada käyttöönsä ylemmän johtoportaan lennokkisuoritteita taisteluunsa liittyen.

Yhtymän taistelua tukevan elektronisen tuen osaston (siis operatiivis-taktisen tason yksikön) tehtävänä on:

- Muodostaa elektroninen tilannekuva yhtymän vastuualueelta paikantamalla vastustajan järjestelmät ja joukot sekä tarvittaessa ja resurssien riittäessä myös omat joukot.

- Paikantaa vastustajan tärkeimmät joukot, erityisesti vastustajan etuosasto, toisen portaan ja reservien sijainti sekä määrittää hyökkäyksen ajoitus ja painopisteen suuntautuminen.
- Antaa uhkavaroitus lentorynnäköstä ilmasuojelutoimenpiteiden toteuttamiseksi sekä antaa ilmatorjunnalle passiivinen maalinosoitus vastustajan lentokoneista ja helikoptereista.
- Antaa uhkavaroitus omassa selustassa toimivista vastustajan tiedustelu-, maahanlasku- tai erikoisjoukoista sekä yhtymän sivustaan kohdistuvista uhkamahdollisuuksista.
- Paikantaa tärkeimmät tulenkäytön maalit kuten divisioonan ja rykmenttien esikunnat ja komentopaikat, tykistön ja raketinheitinten tuliasemat, viesti- ja häirintäasemat sekä tunnistaa maalit omasta tulenkäytöstä johtuvien tappioiden välttämiseksi ja tulen oikeaksi kohdentamiseksi vastustajan kriittisiin pisteisiin.
- Määrittää omalle elektroniselle häirinnälle vastustajan häirittävät maalit ja niiden optimaaliset häirintäparametrit sekä seurata häirinnän vaikutusta operatiivis-taktisella tasalla elektronisen vaikuttamisen toteutuksen ohjaamiseksi.

Verkottuneella taistelukentällä maavoimien sensorit tukevat samalla myös muiden puolustushaarojen tarpeita.

Elektroninen tuki voidaan organisoida usealla eri tavalla: yksi vaihtoehto on toteuttaa organisointi siten, että yksi yksikkö valvoo pintaan (siis vastustajan maavoimia) ja toinen ilmaan (siis vastustajan ilmavoimia ja maavoimien lentojoukkoja). Tämän vaihtoehdon etuna on se, että kummankin järjestelmän käyttöperiaatteet ja toiminta-mallit sekä tekniikka ja henkilöstön koulutus voidaan optimoida kohdejärjestelmiä vastaan. Ilmassa olevat ja ilmapuolustukseen liittyvät kohdejärjestelmät toimivat pääosin tutka- tai UHF-taajuuksilla, kun taas maassa olevat kohteet ilmapuolustuksen tutkia lukuun ottamatta toimivat lähinnä HF-VHF-taajuuksilla. Lentäviä kohteita ovat esimerkiksi vastustajan

- Ilmassa toimivat tutkavalvonta- ja johtokoneet sekä -helikopterit: ilmavalvonta- ja SAR/MTI-tutkat, navigointitutkat, taistelunjohtoyhteydet sekä satelliittiviestiyhteydet.
- Ilma-alusten omatunnistusjärjestelmän (IFF, Identification Friend or Foe) kyselijät ja vastaajat.
- Torjuntahävittäjät, pommi- ja rynnäkkökoneet: monitoimipulssidoppler-, pommitus-, rynnäköinti-, SAR- ja navigointitutkat, ohjusvaroitustutkat, radio-korkeusmittarit, navigointi- ja omatunnusjärjestelmät, omasuojahäirintä-lähettimet, osaston sisäiset yhteydet ja yhteydet taistelunjohtoon sekä tiedustelu- ja tulenjohtokoneisiin.
- Merivalvonta- ja sukellusveneentorjuntalentokoneet sekä tiedustelukoneet: SAR/ISAR- ja vanhemmat muut sivuviistotutkat, taistelunjohtoyhteydet sekä satelliittiviestiyhteydet.

- Taistelu- ja kuljetushelikopterit: millimetriaalto- ja mikroaaltoalueella toimivat tulenjohto-, navigointi- ja/tai törmäysvaroitustutkat, radiokorkeusmittarit, omasuojahäirintälähettimet, maatulenjohtoyhteydet sekä muut yhteydet johtamiseen ja tilannekuvan sekä ennakkovaroitusten välittämiseen.
- Häirintälentokoneet ja -helikopterit: yhteydet osaston johtamiseen ja häirinnän ohjaamiseen sekä häirintälähettimet viesti- ja tutkataajuuksilla.
- Lennokit: komentolinkki ja sensoritiedon välityslinkki suoraan maa-asemaan tai satelliitin välityksellä, sekä lennokissa mahdollisesti oleva aktiivinen hyötykuorma, kuten SAR-tutka tai häirintälähetin.
- Ohjukset: aktiivisella tutkahakupäällä varustetut ilmataistelu- ja meritorjuntaohjukset.

Vastaavasti maassa sijaitsevia kohteita ovat esimerkiksi:

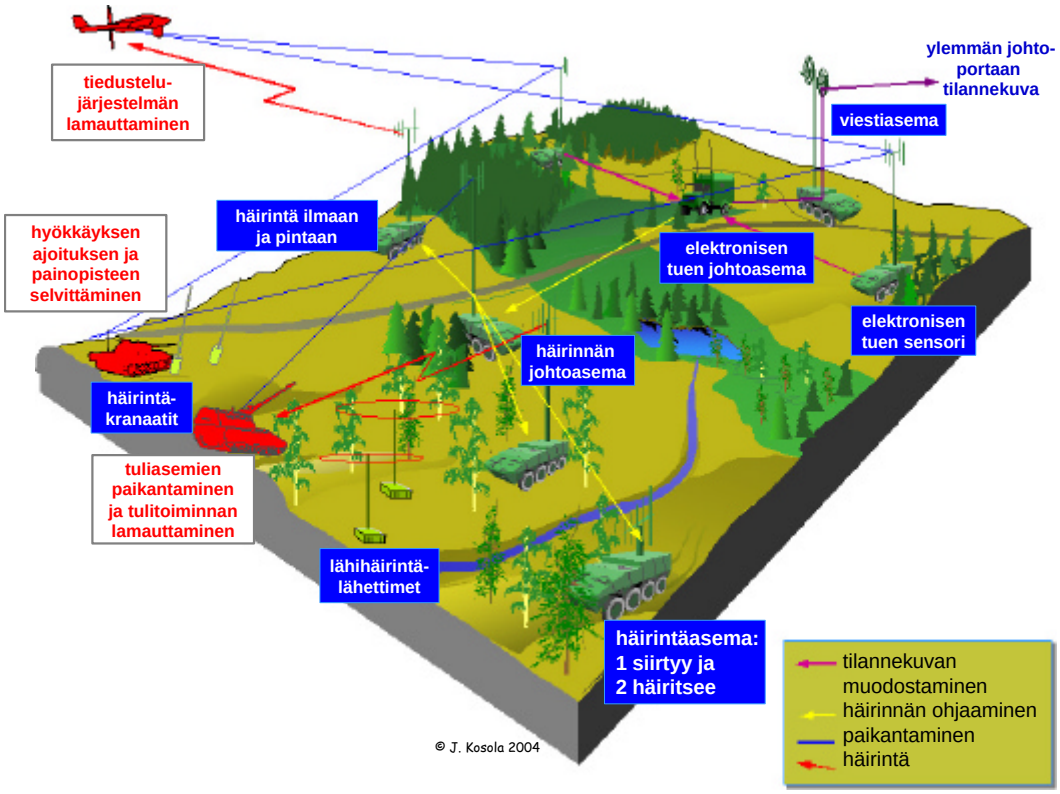
- Komentoradioverkot sekä tiedustelun ja tulenkäytön radioverkot.
- Kenttäradio- ja soluverkkojärjestelmät, erikoisjoukkojen yhteydet HF- ja UHF/SHF- (satellittitietoliikenne) taajuuksilla.
- Mikroaaltoalueen linkkiyhteydet.
- Ilmavalvonta-, taistelunjohto-, vastatykistö-, maastonvalvonta- ja säätutkat sekä ilmatorjuntajärjestelmien erilaiset tutka-, maalinvalaisu- ja omatunnistusjärjestelmät.
- Strategiset viestiyhteydet, mukaan lukien satelliittitietoliikenne.
- Viestihäirintäjärjestelmät, tutkahäirintäjärjestelmät ja näiden johtoyhteydet.

Toinen vaihtoehto on järjestää viestitiedustelun ja elektronisen mittaustiedustelun järjestelmät omikseen vanhan COMINT- ja ELINT-jaon (COMINT = Communications Intelligence, elektroninen viestitiedustelu ja ELINT = Electronic Intelligence, elektroninen mittaustiedustelu) mukaisesti. Viesti- ja elektroninen mittaustiedustelu ovat olleet eriytettyinä koska niiden kohteet, taajuusalueet, laitteistot ja koulutusvaatimukset ovat olleet erilaisia. Joissain maissa tämä on johtanut myös organisaatioiden eriytymiseen. Tilannekuvan muodostamisen kannalta on kuitenkin välttämätöntä yhdistää havainnot mahdollisimman varhaisessa vaiheessa, mikä on helpointa toteuttaa saman organisaation puitteissa. Tämän vaihtoehdon etuna on se, että COMINT-järjestelmä kykenee erikoistumaan vastustajan johtamisjärjestelmän selvittämiseen ja viestiliikenteen kuunteluun ja ELINT-järjestelmä puolestaan vastustajan muiden lähetteiden analysointiin. Haittana puolestaan on se, että samaa kohdetta seuraa ja analysoi kaksi eri järjestelmää ja pahimmassa tapauksessa jopa kaksi eri joukkoa. Kohteesta saatava tieto hajautuu eri tahoille, jolloin johtopäätösten tekeminen ja joissakin tilanteissa uhkavaroituksenkin saaminen riippuu näiden kahden järjestelmän ja joukon välisestä tiedonvaihdosta: esimerkiksi rynnäkkökoneen pommitustutkan havaitsee ELTU/ELINT-järjestelmä tai -joukko, mutta rynnäkkökoneosaston koneiden välisen viestiliikenteen COMINT-järjestelmä tai -joukko.


**Kuva 29: Elektronisen tuen järjestelmä voi olla raskas kuorma-autoihin tai kontteihin asennettu operatiivinen kokonaisjärjestelmä, maastohenkilöautoon asennettu taktinen järjestelmä tai joukon välittömän taistelun tukemiseen soveltuva kevyt kannettava laitteisto**. [ELTA ja Rohde&Schwartz]

Kolmantena vaihtoehtona on sensoreiden tekninen ja organisatorinen integroituminen yhdeksi järjestelmäksi ja yhdeksi joukoksi sekä näin kerätyn sensoritiedon hajauttaminen sitä tarvitseville. Järjestelmien kehitys näyttää olevan menossa tähän suuntaan puolustushaarojen välisen yhteistoiminnan vaatimusten, käytettävissä olevan rahoituksen määrän, taistelukentän verkottumisen asettamien toiminnallisten vaatimusten sekä tekniikan kehittymisen ohjaamana. Tekninen integroituminen johtaa siihen, että taloudellisesti ja teknisesti järkevintä on tarkkailla samalla järjestelmällä kaikkia sähkömagneettiseen spektriin aktiivisesti lähettäviä kohteita. Organisatorisella integroitumisella tarkoitetaan sitä, että puolustushaara-, aselaji- tai toimialakohtaisten joukkoyksiköiden sijasta käytettävissä on kaikkien puolustushaarojen, aselajien ja toimialojen tarpeita palvelevia yhteiskäyttöisiä eli ns. *joint*-yksiköitä. Keskeisimpänä tätä kehitystä hidastavana tekijänä vaikuttaisi olevan muutosvastarinta: ei haluta luopua nykyisin omassa hallinnassa olevasta järjestelmästä ja luottaa yhteiskäyttöisen järjestelmän käytettävyyteen tosipaikan tullen. Tehokkuutta ja suorituskykyä tavoittelevat asevoimat huomaavat ennen pitkää yhteistoiminnan mahdollistaman verkottumisen ja resurssien yhdistämisen mukanaan tuomat mahdollisuudet: nykyaikaisten passiivisten sensorien käyttö pelkästään omasuojaan, tai mihin tahansa muuhun yksittäiseen tehtävään on niiden hukkakäyttöä. Järjestelmät kykenevät vastaanottamaan ja analysoimaan lähes reaaliajassa koko signaalispektrin.

Verkottamalla sensorit omistajasta riippumatta saadaan muuten tarpeettomana hukattava tieto hyötykäyttöön.




**Kuva 30: Esimerkki elektronisen sodankäynnin järjestelmästä maavoimissa, jossa järjestelmäkokonaisuuteen kuuluu elektronisen tuen järjestelmä ja elektronisen vaikuttamisen järjestelmä**

Kuvassa 30 on esitetty esimerkki maavoimien yhtymän elektronisen sodankäynnin järjestelmäkokonaisuudesta. Siihen kuuluu elektronisen tuen järjestelmä, jonka sensoriasemat muodostavat elektronisen tilannekuvan ja häirintäjärjestelmä, joka lamauttaa vastustajan tiedustelu-, valvonta-, johtamis- ja tulenkäytön sensorit tai niiden yhteydet. Häirintäjärjestelmän johtoasema valvoo sensoreillaan häirittäviä vastustajan joukkoja ja ohjaa häirinnän toteuttamista. Kokonaisjärjestelmään kuuluu lisäksi kannettavia ja tykistöllä ammuttavia lähihäirintälähettimiä ja mahdollisesti lennokkeihin ja helikoptereihin asennettuja ELSO-järjestelmiä. Kuva 30 on periaatteellinen eikä esitä mitään tiettyä elektronisen sodankäynnin järjestelmää.

Itse asiassa sensoreiden konvergoituminen on pelkkää elektronista sodankäyntiä laajempi kysymys: yhdistyminen on nähtävissä myös aktiivisten ja passiivisten sensoreiden teknologioiden ja järjestelmien kesken. Tästä käy esimerkkinä amerikkalaisten kehitteillä oleva E-8 JSTARS, E-3 AWACS ja RC-135 Rivet Joint

SIGINT –koneiden seuraaja, joka yhdistää näiden toiminteet osaksi lentävää sensori- ja johtamislavettia E-10A (Future Multi-sensor Command-and-Control Aircraft)[33].

Yhtymän taistelua tukevan taktisen elektronisen häirinnän osaston tehtävänä on

- vastustajan tulikomento- ja tuliasemaviestiliikenteen häirintä
- vastustajan komentoverkon häirintä
- vastustajan tiedustelu- ja tiedustelutulenjohtoviestiliikenteen häirintä
- vastustajan maastonvalvonta- ja vastatykistötutkien häirintä
- vastustajan rynnäkkökoneiden ja taisteluhelikoptereiden tutkien häirintä
- ilmatorjunnan tukeminen vastustajan ilma-alusten johtamisyhteyksien häirinnällä

Häirintä voidaan toteuttaa panssariajoneuvoihin tai telakuorma-autoihin asennetuin häirintälähettimin, alueelta vetäydyttäessä kätketyin tai erikoisjoukkojen toimittamin lähihäirintälähettimin, tykistöllä tai raskaalla raketinheittimellä ammuttavin lähihäirintäkranaatein, lennokkiin tai ilmapalloon sijoitetulla häirintälähettimellä tai jopa viestivälinein, jotka on viritetty vastustajan käyttämille taajuuksille. Häirintäajoneuvoja käytettäessä on aina otettava huomioon se, että vastustaja paikantaa välittömästi häirintäjärjestelmämme omalla elektronisen tuen järjestelmällään ja pyrkii lamauttamaan ne tulenkäytöllä. Tämän vuoksi häirintäajoneuvot toimivat yleensä vaiheittain, esimerkiksi niin, että yksi häiritsee, toinen on valmiina käynnistämään häirinnän johtoaseman käskystä ja kolmas on siirtymässä häirintätehtävän toteuttamisen jälkeen uuteen asemapaikkaansa. Optimaalisin tapa olisi häiritä liikkeestä, mutta tällöin häirintäteho jää vaatimattomaksi, koska häirintäantennia ei voida nostaa riittävän korkealle.

Lähihäirintälähettimet ovat erittäin tehokas tapa lamauttaa vastustajan komentopaikat, tulenjohtoliikenne, radioverkkoihin perustuva tuliasematoiminta sekä elektronisen sodankäynnin sensorit taistelun kriittisimmillä hetkillä[34]. Lähihäirintälähetin voidaan toimittaa tai jättää alueelle erikoisjoukoilla ja ohjelmoida käynnistymään tiettynä ajanhetkenä, tai se voidaan käynnistää radiosignaalilla. Vaikka sen lähetysteho ja antennivahvistus ovat pieniä, tekee lyhyt häirintäetäisyys häirinnästä kuitenkin erittäin tehokasta. Pienikokoista lähihäirintälähetintä tai häirintäkranaattia on käytännössä erittäin vaikeata ja hämärässä sekä peitteisessä maastossa jopa mahdotonta löytää ilman suuntimojärjestelmiä. Jos häirintä toteutetaan siten, että häirintäkranaattien lisäksi ammutaan myös sirpalekranaatteja tai sirotteita, on häirintäkranaattien etsiminen ja raivaaminen erittäin vaikeata ja hidasta. Usein paras keino lähihäirinnän väistämiseksi on siirtyä pois sen vaikutusalueelta. Joskus jo muutaman sadan metrin siirtyminen riittää toimintakyvyn palauttamiseen. Siirtyminen on tällöin varsin pieni vaiva häirinnän väistämiseksi, mutta mikäli kyseessä on tuliportaan, esikunnan tai komentopaikan yllättävä siirto, saattaa puolen tunnin – tunnin toimintakyvyttömyys taistelun kriittisellä hetkellä olla kohtalokasta.

**Kuva 31: Saksalainen Hummel-häirintäajoneuvo. Ajoneuvon katolla on tilaa vievin matalimpien taajuuksien antenniryhmä; korkeampien taajuuksien antennit nostetaan mittaustarkkuuden ja kantaman parantamiseksi maastoesteiden yläpuolelle mahdollisimman korkealle. Korkeimpien taajuuksien pienimmät antennit on sijoitettu radioaaltoja läpäisevään sääsuojaan, *radomiin*. Ylöspäin kapeneva rakenne maston huipussa viittaa päällekkäisiin eri taajuusalueiden antenneihin.** [ewation GmbH/MRCM]

***Merivoimien*** elektronisessa sodankäynnissä korostuu:

- Emissioiden hallinta operaatioturvallisuuden ylläpitämiseksi ja vastustajan maalinosoituksen vaikeuttamiseksi: toiminta passiivisesti joko oman lavetin passiivisen ELTU-sensorin, aktiivisen LPI-tutkan tai muualta tulevan tilannekuvan perusteella.

- Alusten sensoreiden ja asejärjestelmien toimintakyky vastustajan ilmassa ja pinnassa toimivien tausta-, saatto- ja omasuojahäirintäjärjestelmien vaikutuksen alaisena.
- Alusten elektroninen omasuoja(järjestelmä) ja alusosaston suojaaminen (force protection).
- Tukeutumispaikkojen suojaaminen vastustajan asevaikutukselta.

**Kuva 32: Esimerkki aluksen ELTU-järjestelmästä, joka koostuu aluksen mastoihin laitettavista antenneista ja tyypillisesti taistelukeskukseen sijoitetusta vastaanotin- ja analysointijärjestelmästä. Mahdollisimman pitkän kantaman takaamiseksi elektronisen tuen antennit pyritään sijoittamaan ylimmiksi aluksen mastoihin.** [ewation GmbH/MRCM]

Alusten elektronisen tuen järjestelmä on saman tyyppinen ELTU-järjestelmä kuin maavoimienkin laveteissa, mutta luonnollisesti sovitettu merellistä uhkaa vastaan. Se koostuu usein elektronisen tuen sensorista, jonka tehtävänä on havaita alusta uhkaavat muut pinta-alukset, pinta-ajossa olevat sukellusveneet ja lentokoneet ennen kuin niiden tutka kykenee havaitsemaan oman aluksen. Lisäksi elektronisen tuen tehtävänä on antaa uhkavaroitus kohti tulevista aktiivisista tutkahakuisista ohjuksista.

Lasersäteilyyn hakeutuvien ohjusten tai säteenseuraajaohjusten ja pommien yleistymisen myötä alusten omasuojajärjestelmiä ollaan eri maiden merivoimissa täydentämässä myös laservaroittimilla. Omasuojajärjestelmän puolustuslaitteet käsittävät aktiiviset tutkahäirintälähettimet joko aluksella, perässä vedettävällä lautalla, kauko-ohjattavalla miehittämättömällä lavetilla tai rakettiin asennettuna, soihdun- ja silpunheittimet sekä vedettävät ja itsestään liikkuvat harhamaalit. Alusosaston suojaaminen perustuu elektronisen tuen sensorin antamaan tilannekuvaan ja sen perusteella tehtäviin taktisiin ratkaisuihin sekä koko osaston suojaksi käytettäviin omasuojajärjestelmiin.

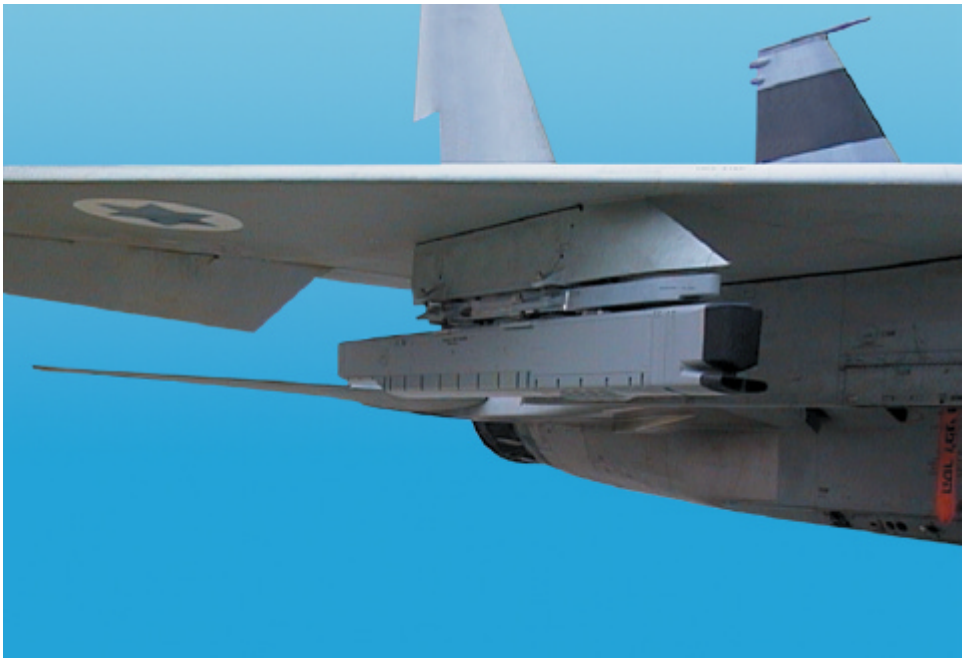
Ilmavoimien suorittamalla häirinnällä voidaan tukea tehokkaasti myös maa- ja merivoimien taistelua. Ilmavoimien elektronisessa sodankäynnissä korostuu usein läheinen suhde fyysiseen asevaikutukseen: ilmavalvonnan ja asejärjestelmien sensoreita on usein helpompi tuhota fyysisesti säteilyyn hakeutuvin ohjuksin kuin häirinnällä. Ilmavoimat voi myös häiritä vastustajan ilmapuolustuksen viestiliikennettä joko ilmassa olevin häirintälähettimin tai toimia maavoimien tapaan, kuten edellä on kuvattu. Lisäksi ilmavoimille on tärkeää täydentää elektronisen tuen sensoreiden avulla tilannekuvaa.

***Ilmavoimien*** elektronisessa sodankäynnissä korostuu

- Emissioiden hallinta: toiminta passiivisesti joko omalta lavetilta tai muualta tulevan tilannekuvan perusteella. Esimerkiksi ruotsalaisessa JAS Gripen -koneessa vastustaja voidaan havaita ja paikantaa passiivisen ELTU-sensorin avulla ilman tarvetta pitää tutkaa aktiivisena. Kaksi tai useampi konetta muodostavat suuntiman vastustajan lentokoneisiin. Vaihtamalla keskenään näitä suuntimia Gripenit kykenevät paikantamaan vastustajan koneet ilman että nämä saisivat varoituksen Gripenin tutkasta omilta tutkavaroittimiltaan[35].
- Johtamisjärjestelmän elektroninen suojaaminen, jotta voidaan varmistaa tilannekuvan välittäminen laveteille ja lavettien välissä[36].
- Lavetin sensoreiden sekä ilmavalvontasensoreiden ja asejärjestelmien toimintakyky vastustajan tausta-, saatto- ja omasuojahäirinnän vaikutuksen alaisena.
- Joukon suojaaminen ilmavalvonta- ja maalinosoitussensoreilta tausta- ja saattohäirinnällä sekä lavettien suojaaminen vastustajan asevaikutukselta omasuojajärjestelmillä.

- Tukikohtien, johtamispaikkojen ja sensoreiden suojaaminen vastustajan asevaikutukselta.

Asejärjestelmien suojaaminen vastustajan elektronisilta omasuojajärjestelmiltä on tärkeätä kaikissa puolustushaaroissa. Asejärjestelmien elektronisen suojan merkitys on kriittinen ilma- ja merivoimille, joiden pääasejärjestelmänä toimivat ohjukset ja pääsensoreina tutkajärjestelmät.



**Kuva 33: Israelilaisen ELTA:n EL/L-8222 -omasuojahäirintäsäiliö ripustettuna F-15-hävittäjäkoneeseen. Taktiset järjestelmät voivat toimia täysin itsenäisesti ilman yhteyttä ohjaajaan (pl. päällä/pois-valinta ja mahdollisesti toimintailmaisin). Vaihtoehtoisesti säiliö on integroitu kiinteästi osaksi muuta koneen sensori-, ase- ja tietokonejärjestelmää.** [ELTA]

Joukon ja lavettien suojaaminen elektronisella häirinnällä ja omasuojajärjestelmillä on edellytyksenä ilmaoperaatioiden käymiselle vastustajan puolustamassa ilmatilassa. Näiden merkitys operaatiomahdollisuuksille sekä operaatioissa syntyvien tappioiden pienentämiselle on keskeinen. Hyvänä esimerkkinä tästä on 1999 Balkanin sota, jossa taustahäirinnän ja omasuojajärjestelmien sekä SEAD/DEAD-koneiden käytön vuoksi serbit onnistuivat ampumaan noin 700 erilaisella ilmatorjuntaohjuksella alas vain kaksi NATO:n lentokonetta[37]. Osa ohjuksista tosin käytettiin lennokkeihin, joita serbit onnistuivat ampumaan alas lukuisia[38].

# 3. ELEKTRONISEN SODANKÄYNNIN LIITYNNÄT MUIHIN TOIMINNAN ALOIHIN

Edellisessä luvussa käsiteltiin elektronisen sodankäynnin elementtejä ja niiden hyödyntämistä taistelussa. Seuraavassa luvussa esitellään elektronisen sodankäynnin tärkeimmät liitynnät muuhun sotilaalliseen toimintaan sekä näiden alueiden mahdollisuudet tukea elektronista taistelua.

## Tiedustelu

Tiedustelulla on keskeinen merkitys asevoimien kyvylle käydä elektronista taistelua: elektroninen tuki luokittelee, yksilöi, paikantaa, tunnistaa, seuraa ja analysoi vastustajan toimintaa sen elektronisten järjestelmien lähettämien signaalien perusteella. Elektronisen tuen järjestelmiin on kuitenkin ohjelmoitava ja niiden operaattoreille on koulutettava spektrin kautta havaittavat signaalit ja niiden ominaisuudet. Elektroninen tilannekuva ja siitä tehtävät arviot muodostetaan yhdistämällä paikannetut ja tunnistetut lähettimet vastustajan järjestelmiin, organisaatioihin ja toimintatapa-malleihin. Tiedustelulla luodaan edellytykset kaikkeen tähän muodostamalla käsitys operaatioalueen joukkojen organisaatiosta, niiden käyttämästä kalustosta ja soveltamista toimintatavoista.

Elektronisen häirinnän vaikuttavuus riippuu voimakkaasti siitä, minkälaisella signaalilla vastustajan järjestelmiä häiritään. Jos häirintäsignaalin teho, pulssin pituus ja pulssien väliaika sekä signaalin taajuus ja muut spektriominaisuudet on sovitettu oikein, häirinnän vaikuttavuus voi olla satoja tai jopa tuhansia kertaluokkia suurempi kuin sokkona toteutetun kohinahäirinnän. Häirintäsignaalin sovittaminen kohde-järjestelmää kohden edellyttää kuitenkin tämän kohdejärjestelmän ominaisuuksien ja ennen kaikkea sen elektronisen suojautumisen toteutusperiaatteiden ja suorituskyvyn tuntemista. Kohdejärjestelmän parametrit on lisäksi ohjelmoitava sekä elektronisen tuen järjestelmiin että elektronisen vaikuttamisen järjestelmiin, jotta kyetään tunnistamaan kohde ja valitsemaan oikeat häirintäparametrit ja -taktiikat.

Elektroninen suojautuminen voidaan toteuttaa elektronista tukea ja vaikuttamista vapaammin uhkariippumattomasti. Kuitenkin myös suojautuminen edellyttää näkemystä elektronisiin järjestelmiin kohdistuvista uhkista, kuten operaatioalueella toimivien tiedustelu- ja valvontajärjestelmien sekä häirintä- ja lamautusjärjestelmien suorituskyvystä ja käyttöperiaatteista. Signaalitiedustelu on keskeisin, muttei suinkaan ainoa tiedustelun liityntä elektroniseen sodankäyntiin. Siitä lisää seuraavassa.

## Signaalitiedustelu

Signaalitiedustelu (SIGINT, Signals Intelligence) on strategiseen tiedustelun kuuluvaa vastustajan sähkömagneettisiin signaaleihin kohdistuvaa tiedustelua, jonka tarkoituksena on havaita vastustajan sähkömagneettisen spektrin käyttö, analysoida, luokitella ja tunnistaa vastustajan lähetteet sekä luokitella, tunnistaa, yksilöidä ja paikantaa vastustajan elektroniset järjestelmät. Havaitut lähetteet pyritään assosioimaan vastustajan järjestelmiin ja joukkoihin. Samoin lähetteiden kautta havaittava toiminta pyritään liittämään vastustajan toimintatapaan.

**Kuva 34: Esimerkki aluksen signaalitiedustelujärjestelmästä. Eri taajuusalueiden suunnanmittaukseen kykenevät antennit sijoitetaan korkealle mastoon, käyttökonsolit yleensä aluksen taistelukeskukseen.** [ewation GmbH/MRCM]

Signaalitiedustelun antamia tietoja käytetään yhtenä tiedustelulähteenä vihollistilannekuvan muodostamisessa, uhkavaroituksessa, omien vastatoimenpiteiden valmistelemisessa sekä omien vaikutustoimenpiteiden vaikutuksen arvioimisessa. Signaalitiedustelusta ja elektronisesta tiedustelusta voidaan tiedustelun kohteen perusteella käyttää nimityksiä elektroninen viestitiedustelu (COMINT, Communications

Intelligence) tai elektroninen mittaustiedustelu (ELINT, Electronic Intelligence). Edellinen kohdistuu viestijärjestelmiin ja jälkimmäinen tutkiin ja muihin järjestelmiin.

Signaalitiedustelussa käytetään samoja menetelmiä ja joissakin tilanteissa jopa samoja laitteita kuin elektronisessa sodankäynnissä. Sitä ei kuitenkaan lueta elektronisen sodankäynnin osaksi, sillä sen katsotaan olevan osa strategista tiedustelua. Signaalitiedusteluun liittyvän tiedon luottamuksellisuusvaade on yleensä suurempi tiedustelun lähdesuojan vuoksi[39] kuin kriisiaikaan painottuvan elektronisen tuen.

Vaikka signaalitiedustelussa käytettävä teknologia ja sovellettava menettelytavat ovatkin monelta osin yhteneviä elektronisen tuen kanssa, edellä kuvattu jako perustuu myös tiedon hyödyntämiseen: strategisen tiedustelun tietoja hyödynnetään mm. valtakunnallisessa varautumisessa, joten siihen liittyvä toiminta on luonteeltaan pitkäaikaista ja aikaa vievää. Operatiivisen elektronisen tuen tietoja hyödynnetään mm. operaatioiden suunnittelussa ja toteuttamisessa huomattavasti lyhyemmällä aikajänteellä: tiedustelun osalta päivistä tunteihin ja maalinosoituksen osalta minuuteista sekunteihin.

Signaalitiedustelua voi järjestelmiämme vastaan kohdistua esimerkiksi:

- Valtakunnan rajojen läheisyydessä sijaitsevilta kiinteiltä tiedusteluasemilta, jotka on varustettu korkein mastoin ulottuvuuden maksimoimiseksi.
- Valtakunnan rajan läheisyydessä tai kansainvälisessä ilmatilassa lentävistä signaalitiedustelukoneista tai kansainvälisellä merialueella liikkuvista tiedustelualuksista.
- Avaruudessa toimivista signaalitiedustelusatelliiteista.

Signaalitiedustelu-uhka on siten otettava huomioon paitsi sodan ajan taistelutoiminnassa, myös:

- Rauhanaikaisessa järjestelmien testauksissa ja kenttäkokeissa.
- Joukkojen koulutuksessa ja sotaharjoituksissa.
- Joukkojen perustamis- ja ryhmittämisvaiheessa.
- Joukkojen perustamisen jälkeisessä koulutuksessa ja harjoituksissa, erityisesti todellisten operaatioajatusten mukaisissa harjoituksissa.

Signaalitiedustelua ei käsitellä tämän laajemmin, koska se ei kuulu kirjan aihepiiriin. Lukijan toivotaan kuitenkin muistavan, että meihin kohdistuu signaalitiedustelu-uhka koko ajan, ja että rauhan aikaisella tiedustella luodaan pitkälti edellytykset kriisitilanteessa meihin kohdistuvalle ELSO-uhkalle. Siten suojautuminen vastustajan signaalitiedustelulta tuo suojaa myös kriisinaikaiselta elektroniselta sodankäynniltä. Koska signaalitiedustelu on sen kohteelle näkymätöntä, sen muodostama uhka unohtuu varsin helposti.

# Taajuushallinta

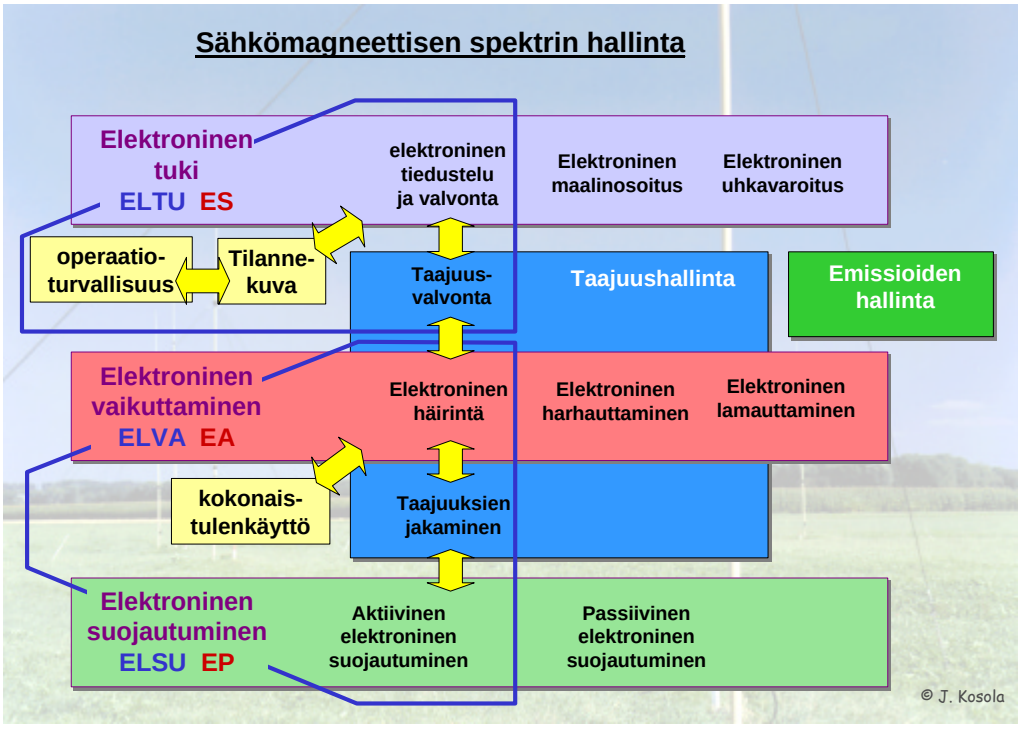
## Taajuushallinnan rooli sotilaallisissa operaatioissa

Asevoimien ja yhteiskunnan suuri riippuvuus sähkömagneettista spektriä hyödyntävistä järjestelmistä sekä elektronisella taistelukentällä oleva suuri elektronisten laitteiden määrä korostavat taajuushallinnan keskeistä asemaa taistelukentällä. Puolustushaarojen yhteistoiminta ja järjestelmien taistelunkestävyys edellyttävät joustavaa ja reaaliaikaista taajuushallinnan johtamista. Suomalaisessa käsitemaailmassa taajuushallinta ei ole osa elektronista sodankäyntiä. Kuitenkin esimerkiksi NATO:n ja Yhdysvaltain asevoimien mukaan taajuuksien käytön ohjaus (frequency deconfliction) sekä suojautuminen myös omilta elektronisen sodankäynnin menetelmiltä on osa elektronista suojautumista[k]. Operatiivisen käytön kannalta on huomattava, että häiriösignaalin vuoksi toimimaton järjestelmä on toimimaton, vaikka häiriö tulisikin omista järjestelmistä.

Elektronisessa sodankäynnissä on kyse sähkömagneettisen spektrin hallitsemisesta – omien joukkojen ja järjestelmien spektrin käyttö on mahdollistettava ja vastustajan kykyä käyttää sähkömagneettista spektriä hyväkseen on heikennettävä. Nämä vaatimukset ovat toisinaan ristiriitaisia: vastustajan järjestelmien häirintä saattaa vaikuttaa omien joukkojen toimintakykyyn, mikäli niiden järjestelmät toimivat samalla taajuuskaistalla. Toisaalta omien taajuuksien käytössä on jo etukäteen otettava huomioon mahdolliset tulevat tarpeet häiritä näitä taajuuksia. Tämä tieto puolestaan saadaan etukäteen ELSO-tukitoiminnan välittämänä signaalitiedustelulta ja taistelujen aikana reaaliaikaisesti elektroniselta tuelta (ELTU).

Sodan ja kriisin aikana taajuushallinta on osa elektronisen taistelun suunnittelua ja johtamista. Taajuushallinnalla luodaan mahdollisuuksia käyttää taajuuksia, ja elektroniseen suojautumiseen liittyen pyritään osoittamaan näistä käyttöön soveltuvia taajuuksia ja toimintamoodeja, joilla toiminta vastustajan tiedustelu-, valvonta-, maalinosoitus- ja häirintäuhkan alla on mahdollista. Taajuushallinnalla pyritään valvomaan omien joukkojen taajuuksien käyttöä allokointi- ja käyttökonfliktien havaitsemiseksi. Elektronisella tuella puolestaan pyritään muodostamaan kokonaistilannekuvaa riippumatta siitä onko informaation lähde vastustajan, kolmansien osapuolten, tai omien joukkojen käyttämä järjestelmä. Elektronisella vaikuttamisella pyritään estämään vastustajan järjestelmien kykyä käyttää sähkömagneettista spektriä. Vaikuttamisessa on otettava huomioon paitsi se, miten vastustajan operatiivinen kyky tietyistä spektrin osista riippuu, myös se, että häiritsemällä voidaan samalla estää tai haitata omaa kykyä hyödyntää spektriä sekä oman tiedustelujärjestelmän toimintaa.

[k] Puhuminen taajuushallinnasta on jossain määrin harhaanjohtavaa, sillä kyseessä ei ole pelkkä taajuuksien jakaminen käyttöön, vaan osin jo nykyisin taajuushyppivien (FH, frequency hopping) järjestelmien hypintäkoodia on kyettävä ohjaamaan siten, etteivät järjestelmät häiritse toisiaan. Tulevaisuudessa samoilla taajuusalueilla toimivien CDMA-tyyppisten (code division multiple access) järjestelmien yleistyminen ohjaa taajuushallintaa myös hajaspektrikoodien hallinnan suuntaan.




**Kuva 35: Sähkömagneettisen spektrin hallintaan kuuluu osia elektronisesta sodankäynnistä, taajuushallinta ja emissioiden hallinta. Taajuushallinnan elementeistä taajuuksien käyttöön jakaminen sekä taajuusvalvonta liittyvät läheisesti elektroniseen sodankäyntiin. Taajuuksien jakaminen on suunniteltava yhdessä elektronisen häirinnän ja kokonaistulenkäytön suunnittelun sekä elektronisen suojautumisen kanssa. Näitä on tarvittaessa kyettävä myös johtamaan yhdessä. Vastaavasti taajuusvalvonta ja elektroninen tiedustelu ja valvonta muodostavat yhdessä spektrin kokonaisvalvonnan, joka palvelee sekä omien että vastustajan ja kolmansien osapuolten käyttämien taajuuksien valvontaa.**

Elektronista taistelua johdettaessa on kyettävä tarvittaessa reaaliaikaisesti arvottamaan, onko vastustajan kriittisten järjestelmien häiritsemisen antama lisäarvo omalle operaatiolle merkittävämpi kuin vaikkapa joidenkin omien tiedustelu- tai johtamisjärjestelmien lamautumisen aikaansaama suorituskyvyn heikkeneminen.

Taajuushallinnalla on keskeinen rooli myös elektronisen harhauttamisen toteuttamisessa. Ase- ja sensorijärjestelmien suojaamiseksi taistelukentälle kannattaa luoda niitä muistuttavia halpoja harhamaalilähettimiä. Reaaliaikaisella taajuus-hallinnalla voidaan tällöin synnyttää hämmennystä vastustajan tiedustelujärjestelmään vaihtelemalla harhamaalijärjestelmien ja todellisten järjestelmien taajuuksia ja muita signaaliparametreja.

Näiden sidosten ja reaaliaikavaatimusten vuoksi kriisin aikana taajuushallinnan on oltava osa elektronisen taistelun suunnittelua ja johtamista ja sen on perustuttava

jatkuvasti päivittyvään elektroniseen taistelusuunnitelmaan, jossa huomioidaan omien joukkojen elektronisen suojan tarve, elektronisen tuen antamat tilanne- ja vihollistiedot sekä oma tiedustelu- ja häirintätarve. On myös harkittava, olisiko kaikki sähkömagneettisen spektrin hallintaan liittyvät toiminteet ja voimavarat keskitettävä samaan organisaatioon.

Taajuuksien sotilaallista käyttöä rajoittavat hyvin suuressa määrin yhteiskunnan muut tarpeet ja erilaiset kansainväliset sitoumukset. Nykyaikainen tietoyhteiskunta tarvitsee suuria osia sähkömagneettisesta spektristä ja on ne myös varannut käyttöönsä. Rauhan ja sodan ajan spektrinkäytön optimoiminen siten, että kyetään takaamaan yhteiskunnan toiminta normaalioloissa, täyttämään kansainväliset velvoitteet ja varmistamaan yhteiskunnan kriittisen infrastruktuurin sekä puolustusjärjestelmän toiminta sodan ajan oloissa edellyttävät, että:

- Taajuuksien jakamisessa otetaan huomioon yhteiskunnan ja puolustusvoimien kriisiajan tarpeet.
- Määritellään puolustusvoimille sellaiset taajuuksien käyttöoikeudet, jotka mahdollistavat rauhan ajan harjoittelun sekä alueellisen koskemattomuuden valvonnan ja turvallisuuden normaalioloissa ja joilla taataan järjestelmien toimintakyky kriisiajan elektronisella taistelukentällä.
- Vastustajan järjestelmien suorituskyky ja mahdolliset heikkoudet ennakoidaan ja otetaan järjestelmäsuunnittelussa huomioon. Taajuushallinnan vaatimukset ja optimointiratkaisut otetaan huomioon materiaalihankkeiden hankevaihtoehtoja arvioitaessa, esiselvitysvaiheissa ja vaatimusmäärittelyissä.
- Omalle toiminnalle ja toimintaympäristön muille sotilas- tai siviilijärjestelmille aiheutuvat häiriöt ennakoidaan ja hallitaan.
- Voimankäyttöprofiileihin määritetään sähkömagneettisen spektrin käyttöön liittyvät voimankäytön oikeudet.
- Valmius- ja puolustustilalaissa kuvataan miten yhteiskunnan ja puolustusvoimien spektrinkäyttövalmiuksia lisätään uhkaa vastaavasti strategisen iskun ja laajamittaisen hyökkäyksen torjuntakyvyn luomiseksi.
- Rauhan aikaiset järjestelmien ominaisuuksien ja toimintatapojen salaamiseen liittyvät käyttörajoitukset sekä koulutus- ja testaustoiminta ohjeistetaan elektronisen suojautumisen edellyttämällä tavalla.

## Taajuushallinnan toteutus puolustusvoimissa rauhan aikana

Puolustusvoimien taajuushallinta on ohjeistettu Pääesikunnan johtamisjärjestelmäosaston ohjeessa Puolustusvoimien radiohallinto[40]. Puolustusvoimien taajuushallinnan tehtävä on täyttää sotilaallisen maanpuolustuksen radiotoiminnan asettamat taajuustarpeet kaikissa valmiustiloissa. Sähkömagneettinen spektri on rajallinen luonnonvara: vaikka spektri ei käytössä kulukaan, sitä ei myöskään voida valmistaa lisää eikä käytettävää spektriä voida luonnonlakien ja toimintaympäristön asettamien rajoitusten vuoksi laajentaa loputtomiin. Siten taajuuksien koordinoitu hallinta on keskeisen

tärkeätä sekä asevoimien että koko yhteiskunnan toiminnan kannalta. Taajuushallinnalla varmistetaan taajuuksien tarkoituksenmukainen käyttö:

- eri toimijoiden mahdollisuus käyttää samanlaisia järjestelmiään samoilla toiminta-alueilla
- eri toimijoiden ja eri järjestelmien aiheuttamien häiriöiden välttäminen, oli sitten kyseessä itselle tai toisille aiheutuvat häiriöt
- taajuusvarojen (käyttöön saatujen taajuuksien) käytön optimointi

Esimerkkejä, joiden kaltaisiin tilanteisiin taajuushallinnan laiminlyönti voi johtaa:

1. Hankitaan radiolaitteita varmistamatta, että samalle operaatio-alueelle ryhmitettävät sadat radiot voivat toimia häiritsemättä toisiaan.
2. Hankintaan järjestelmä, jonka käyttämät taajuudet ovat kokonaan tai pääosin yhteiskunnan muuhun käyttöön varaamalla taajuus-alueella, eikä järjestelmää voi käyttää koulutuksessa kuin rajoitetuilla syrjäisillä alueilla.
3. Järjestelmän kenttäkokeissa paljastetaan elektronisen suojau-tumisen vaarantavia ominaisuuksia, kuten järjestelmän käyttämän taajuuskaistan todellinen laajuus.
4. Hankitaan järjestelmä, jonka lähettimet muodostavat helposti tunnistettavan kokonaisuuden.
5. Hankitaan järjestelmä, joka toimii taajuusalueella, jota on suunni-teltu uhkakuvan mukaisesti häirittäväksi.
6. Kohdennetaan kullekin järjestelmälle oma erillinen taajuus-kaistansa, jolloin vastustajan elektroninen tiedustelu kykenee suoraan päättelemään järjestelmän sen käyttämän taajuuden perusteella
7. Hankitaan järjestelmä, jonka käyttö lamauttaa oman omasuoja-järjestelmän toiminnan.
8. Joukon johtaja ei voi määrittää ongelmatilanteessa uusia käytet-täviä taajuuksia silloin kun käyttöön annetut taajuudet tulevat häirityiksi.

**Taulukko 2: Esimerkkejä taajuushallinnan laiminlyönnistä eri tilanteissa. Kuten esimerkeistä käy ilmi, taajuushallinnalla on yhteys paitsi elektroniseen sodan-käyntiin, myös järjestelmien keskinäisen sähkömagneettisen yhteensopivuuden varmistamiseen[41].**

Taajuuksien käytön määrittelee maailmanlaajuisesti YK:n alainen WRC (World Radio Conference), jonka päätökset ovat velvoittavia. Kansalliset taajuuksien jakoon liittyvät päätökset perustuvat radio- ja viestintälainsäädäntöön. Suomessa Viestintävirasto on

laissa määritelty viranomainen, jolla on toimivaltuudet jakaa taajuuksia käyttöön ja joka pitää yllä radiotaajuuksien käyttösuunnitelmaa. Myös puolustusvoimat toimii Viestintäviraston asettamissa puitteissa.

Viranomaisille ja elinkeinoelämälle on annettu käyttöön taajuuskaistoja niiden myöntämisluvissa mainituin ehdoin ja vahvistettuja taajuusmaksuja vastaan. Puolustusvoimat hallitsee sotilaalliselle maanpuolustukselle annettuja taajuusalueita, jotka tarkastetaan vuosittain[42]. Rauhan aikana taajuushallinnassa korostuu[43]:

- Toimintatilan raivaaminen elektroniselle taistelukentälle. Tällä tarkoitetaan hallinnollisia menettelyitä, joilla varmistetaan riittävän laajojen spektrin osien käyttöoikeudet rauhan ja kriisin aikaisessa toiminnassa ja toimintavalmiudessa.
- Yhteiskunnan kriittisen infrastruktuurin ja puolustusvoimien sodan ajan toimintakyvyn varmistaminen luomalla jo rauhan aikana sotilas- ja siviiliviranomaisten riittävän kattava ja nopea yhteistyö taajuuksien käytölle poikkeusoloissa.
- Tiedustelu-, valvonta-, johtamis-, omasuoja-, omatunnistus-, navigointi- ja ase-järjestelmien järjestelmäarkkitehtuurien suunnittelu siten, että kokonais-järjestelmään kuuluvat laitteet käyttävät sellaisia spektrin osia, joilla voidaan taata edellytykset rauhan aikaiseen koulutukseen ja valmiuden ylläpitoon sekä joilla on riittävän laaja toimintavapaus kriisin aikana.
- Spektriä tehokkaasti käyttävien tekniikoiden ja menetelmien kehittäminen ja käyttöönotto. Kaikkien kehitettävien järjestelmien tulee olla sellaisia, jotka sietävät muita järjestelmiä ja jotka häiritsevät mahdollisimman vähän toisia sähkömagneettisessa spektrissä.
- Spektrin käytön osaamisen lisääminen puolustusvoimissa.
- Puolustusvoimien spektrinkäyttöoikeuksien varmistaminen kansallisilla ja kansainvälisillä foorumeilla.
- Kattavan spektrinkäyttösuunnitelman laadinta ja ylläpito, joka sisältää sekä puolustusvoimien nykyisen spektrin käytön että suunnitellut tulevaisuuden tarpeet.
- Maanpuolustuksen suorituskykyyn syntyvien rajoitusten ja haavoittuvuuksien ymmärtäminen tilanteissa, joissa spektrin tietyt osat eivät ole puolustusvoimien järjestelmien käytettävissä.

Puolustusvoimissa taajuushallinnan ohjaamisesta vastaa Pääesikunnan johtamis-järjestelmäosasto (PEjojä-os), joka määrittää yleisjärjestelyt ja vastuut sekä neuvottelee taajuuksien saamisesta sotilaskäyttöön. Taajuushallinnan käytännön toteuttamisesta vastaa Pääesikunnan alainen Puolustusvoimien Tietotekniikkalaitos, joka ylläpitää taajuustilannekuvaa ja taajuuksien käytön tietopankkia sekä jakaa käyttöön puolustusvoimien käyttöönsä saamat sotilastaajuusalueet. Maanpuolustusalueet ja

puolustushaarat vastaavat taajuushallinnan toteuttamisesta alueellisesti ja toimialoittain[1].

Yksityiskohtaiset vastuut ja oikeat menettelyt eri tilanteissa käyvät ilmi pysyväisasiakirjoista ja niiden soveltamisohjeista. Järjestelmien toimintaedellytysten ja elektronisen suojautumisen kannalta on kuitenkin tärkeätä, että järjestelmien hankinnan yhteydessä varmistetaan normaalin taajuuslupamenettelyn lisäksi ainakin:

- Kyseiselle taajuuskaistalle rauhan ja sodan aikana käyttöön saatava taajuusalue ja sen riittävyys sekä rauhan ajan koulutuskäyttöön että sodan ajan toimintaan vastustajan tiedustelu- ja häirintäuhan alla.
- Miten kyseisen taajuusalueen käyttö on mahdollista kriisiaikana: mitä muita omia ja mitä vastustajan järjestelmiä alueella sijaitsee ja miten ne häiritsevät toisiaan?
- Miten oma ja vastustajan elektroninen häirintä kyseisellä taajuusalueella toimii?

## Häivetekniikka ja elektroninen sodankäynti

Häivetekniikka on teknologian alue, joka tukee elektronista suojautumista. Erilaisin häiveteknisin ratkaisuin voidaan minimoida suojattavan kohteen herätteet, erityisesti tutkakaiku ja lämpöheräte. Hyvästä häiveteknisestä toteutuksesta huolimatta kohde voi kuitenkin paljastua elektroniselle tiedustelulle huonosti suojattujen elektronisen järjestelmien, kuten tutkan, viestijärjestelmän, radiokorkeusmittarin, laseretäisyysmittarin tms. vuoksi. Vastaavasti järjestelmän suojaaminen elektroniselta tiedustelulta ei paljoa auta, mikäli järjestelmä kuitenkin paljastuu vaikkapa vastustajan SAR-tutkaukselle suuren ja helposti erottuvan tutkakaikunsa vuoksi.

Tutkataajuusalueen häivetekniikka tulee huomioida lavettien suunnittelussa ja hankinnoissa. Yksinkertaisilla muotoilullisilla ratkaisuilla voidaan saada aikaan suuri hyöty, joskin varsinaisen tutkassa lähes näkymättömän lavetin tekeminen on sangen kallista. Infrapuna-alueella lämpöherätteen minimoiminen tai taustan kaltaiseksi muokkaaminen on tutkataajuusalueen häivetekniikkaa halvempaa, minkä vuoksi lämpöherätteen minimointi on perusteltua huomioida kaikessa lavetti- ja varustesuunnittelussa.

Häivetekniikka on nähtävä omasuojan lisäksi myös hyökkäyksellisenä tekniikkana. Herätteiden pienentäminen voi tukea häirintää tai riittää yksin esim. pommitustehtävissä siihen, että vastustajan ilmapuolustukseen saadaan riittävä aukko hyökkäysosaston viemiseksi läpi puolustusketjun. Häivetekniikka yksinään ei riitä ajoneuvojen

[1] Puolustusvoimien tulevien johtamisjärjestelmä- ja organisaatiomuutosten myötä maanpuolustusalueet lakkautetaan ja Tietotekniikkalaitoksen korvaa perustettava johtamisjärjestelmäkeskus.

tai pinta- tai ilma-alusten suojaamiseen, vaan sitä on käytettävä yhdessä elektronisen sodankäynnin menetelmien kanssa[44].

**Kuva 36: Järjestelmän suoja elektronista valvontaa vastaan perustuu emissioiden hallintaan, jonka yksi osatekijä on elektroninen hiljaisuus. Lisäksi on kuitenkin kyettävä suojautumaan myös visuaaliselta tiedustelulta sekä lämpö- ja tutka-tiedustelulta.** [SA kuva]

Elektronisen tuen sensorilla on keskeinen merkitys häivekohteiden tilannetietoisuuden ylläpitämisessä. Tutka pilaisi häivetekniikan tuoman edun, koska aktiivisena sensorina se on havaittavissa elektronisen tuen keinoin, vaikka vastustajan tutkajärjestelmä ei havaitsisikaan kohdetta. Passiivisella ELTU-sensorilla varustettu häivekone (tai -alus) voi sen sijaan itse havainnoida ympäristöään mutta pysyä elektronisessa hiljaisuudessa ja siten vastustajan tutkien ja passiivisten sensoreiden havaitsemattomissa. Tällöin häivekone voi kiertää havaitsemansa valvonta- ja maalinosoitustutkat niin kaukaa, että kykenee pysyttelemään häivetekniikan avulla näiden havaitsemattomissa.

## Harhautus elektronisen sodankäynnin tukena

Harhautuksella on keskeinen merkitys sodankäynnissä, ja niin myös elektronisessa sodankäynnissä. Toimiakseen harhautus edellyttää sen pitämistä salassa. Siten myös harhautukseen liittyvät ohjeet ja toiminta-ajatukset on pidettävä salassa. Jotta lukijalle kuitenkin syntyisi jonkinlainen käsitys siitä, minkälaisiin tarkoituksiin ja minkälaisin keinoin harhautus tukee elektronista sodankäyntiä, on tähän sisällytetty lyhyt ylimalkainen kuvaus. Sen tavoitteena on herättää lukijan omia ajatuksia siitä, miten harhauttamista voitaisiin soveltaa todellisessa toiminnassa tukemaan elektronisen sodankäynnin eri elementtejä. Esimerkit perustuvat julkisiin lähteisiin ja sen vuoksi

pitkälti historian tapahtumiin. Nykyisissä suunnitelmissa ja toiminta-ajatuksissa lukijan tulee tukeutua asianomaiseen tietoturvaluokiteltuun materiaaliin. Harhautuksen yhteydessä on lisäksi aina muistettava, että vastustajan tiedustelujärjestelmät käyttävät useita eri tiedon lähteitä oman käsityksensä muodostamiseen. Tällä pyritään sekä kompensoimaan epäluotettavien ja epätäydellisten lähteiden merkitystä että erottamaan tosiasiat harhautuksesta.


**Kuva 37: Lockheed Martinin F/A-22A Raptor nousee ilmaan Edwardsin lentotukikohdasta USA:ssa. Eräässä ilmataisteluharjoituksessa häivetekniikalla toteutettu Raptor kykeni tuhoamaan kolmessa minuutissa viisi F-15 ilmaherruushävittäjää ilman että nämä edes havaitsivat FA-22:ta.** [© Jane's 2004]

## Harhautus elektronisen tiedustelun ja valvonnan tukena

Harhautuksella voidaan estää vastustajaa päättelemästä, että sen toiminta paljastuu elektroniselle tiedustelulle ja valvonnalle. Jos vastustaja ei epäile toimintansa paljastuneen elektronisen tuen sensoreille, se ei myöskään ymmärrä muuttaa toimintatapaansa sellaiseksi, joka heikentäisi elektronisen tuen kykyä kerätä tietoa vastustajasta. Tunnetuin esimerkki tästä on brittien toiminta saksalaisten sukellusveneitä vastaan Atlantilla toisessa maailmansodassa. Britit kykenivät saksalaisiin verrattuna ylivoimaisen elektronisen sodankäynnin kykynsä avulla sieppaamaan Kriegsmarinen viestiliikenteen ja purkamaan saksalaisten käyttämän salauksen. Tämä signaalitiedustelun ja kryptoanalyysin yhdistelmä mahdollisti saksalaisten operaatioajatuksen selvittämisen sekä sukellusveneentorjuntakoneiden suuntaamisen veneiden toimialueelle. Tämän jälkeen sukellusveneiden HF-viestiliikenteen suuntimisen perusteella oli mahdollista paikantaa pinnalla olevat veneet karkeasti ja suunnata tutkalla varustettujen lentokoneiden hyökkäyksiä niitä vastaan. Jotta toimintamalli ei

olisi paljastunut saksalaisille, britit lähettivät yleensä alueelle ensin merivalvontakoneita, jotta saksalaiset olisivat arvelleet brittien menestyksen johtuvan näiden tekemistä havainnoista. Saksalaiset epäilivät brittien paikantavan heidän sukellusveneensä tutkalla, mikä johti huomion kiinnittämiseen tutkasäteilyä absorboiviin materiaaleihin. Esimerkki kuvaa harhautuksen roolia strategisen tason taistelussa, mutta ajatusmalli pätee myös operatiivisella ja taktisella tasolla.

***Elektronisen tiedustelun ja valvonnan suorituskyvyn tukemiseksi on edullista harhauttaa vastustaja kuvittelemaan, että tieto on saatu jollakin toisella keinolla, kuten partiotiedustelulla, aktiivisella sensorilla, tai jollakin muulla tiedustelumenetelmällä.***

## Harhautus elektronisen vaikuttamisen tukena

Kuten aiemmin on esitetty, elektronisella vaikuttamisella kyetään supistamaan järjestelmien toiminnallista kantamaa sekä rajoittamaan niiden toiminta-alueita, mutta harvoin lamauttamaan ne täysin. Mikäli vastustaja suunnittelee toimintansa jo alun perin siten, että ottaa huomioon toisen osapuolen suorittaman häirinnän, voi se taata järjestelmiensä toiminnan ainakin painopistealueilla. Vastaavasti toimimaton viestijärjestelmä on usein saatavissa toimivaksi elektronisen suojautumisen keinoin, kuten käyttämällä pitkälanka-antennia, lyhentämällä yhteysetäisyyksiä tms. Tämä kuitenkin edellyttää, että vastustaja osaa päätellä järjestelmiensä toimimattomuuden johtuvan elektronisesta vaikuttamisesta. Tämän vuoksi elektroninen vaikuttaminen tehoaa pidempään, mikäli sen kohde ei havaitse olevansa elektronisen vaikuttamisen piirissä (tästä käytetään nimitystä black jamming). Sen vuoksi häirintä voi joissakin tilanteissa tehota pidempään, mikäli sillä ei estetä kaikkea viestiliikennettä, vaan muutetaan viestien sisältöä, syötetään kokonaan itse kehitettyjä harhauttavia sanomia tai estetään vain tärkeimpien sanomien tai sanoman kriittisen osan välittäminen. Kohdejärjestelmien salauksen kehittyminen sekä häirintäjärjestelmien automatisoituminen ja niiltä vaadittavan reagointiajan lyheneminen tosin heikentävät edellytyksiä tämän kaltaisen valikoivan häirinnän toteuttamiseen.

Vastustaja voidaan myös totuttaa häirintätilanteeseen vähä vähältä niin, ettei se havaitse olevansa häirinnän kohteena. Esimerkiksi saksalaiset totuttivat talvella 1942 brittien tutkaoperaattorit häiriötasoon, jota kohotettiin asteittain aina tiettyyn vuorokauden aikaan. Tämä heikensi tutkien kantamaa brittien sitä havaitsematta niin, että Brestissä Ranskassa olleet taisteluristeilijät Scharnhorst ja Gneisenau sekä raskas risteilijä Prinz Eugen kyettiin siirtämään englantilaisten silmien edessä Englannin Kanaalin läpi Saksaan.

## Harhautus elektronisen suojautumisen tukena

Elektroniseen suojautumiseen liittyy keskeisesti suojautuminen järjestelmiä, joukkoja ja toimintatapoja vastaan kohdistuvalta tiedustelulta ja valvonnalta. Harhauttamisella tuetaan elektronista suojautumista tavoitteena joko vaikeuttaa vastustajan

valmistautumista elektroniseen valvontaan ja häirintään tai vaikeuttaa vastustajan tiedustelua. Esimerkiksi Yhdysvaltain asevoimien elektronisen sodankäynnin doktriini (US joint EW doctrine) sisällyttää tällaisen harhauttamisen osaksi viestiturvallisuutta (COMSEC, communications security)[45]. Ensin mainitussa tarkoituksessa vastustajalle voidaan syöttää tarkoituksellisesti vääriä tietoja järjestelmiemme tekniikasta ja käyttöperiaatteista sekä joukkojen toiminnasta. Tavoitteena voi tällöin olla saada vastustaja kehittämään omia ELSO-järjestelmiään siten, että niistä on vähemmän uhkaa omalle toiminnallemme esimerkiksi kiinnittämällä vastustajan huomio valheellisiin teknisiin heikkouksiin, vääriin ominaisuuksiin tai toimintatapamalleihin yms. Vastustajalle voidaan syöttää eri tiedotusvälineiden kautta esimerkiksi kuva todellista kapeammasta tai jopa kokonaan väärästä taajuusalueesta. Vastaavasti mahdolliset todelliset heikkoudet pyritään estämään, esimerkiksi mikäli jokin asejärjestelmä sisältää vain satelliittipaikannuslaitteen ja olisi siten altis elektroniselle häirinnälle, luodaan illuusio siitä, että järjestelmässä on varalla inertiasuunnistus, joten elektroninen häirintä ei olisi tehokasta. Jos tällä saadaan vastustaja luopumaan häirintämenetelmän kehittämisestä, on asejärjestelmä saatu suojattua vastustajan häirinnältä ilman minkäänlaisia elektronisia suojautumiskeinoja.

Vastustajan tiedustelun vaikeuttamiseksi voidaan sille syöttää harhauttavaa tietoa erityisesti vastustajan tiedustelulle alttiiden viestijärjestelmien kautta. Tällöin vastustaja ei kykene suoraan hyödyntämään viestijärjestelmän tiedustelun kautta saamiaan tietoja, vaan sen on aina otettava huomioon mahdollisuus, että tiedot ovatkin harhautusta ja se joutuu varmistamaan niiden todenperäisyyden muista tiedustelulähteistä. Tämä hidastaa vastustajan tiedustelua ja saattaa parhaassa tapauksessa saada sen tekemään vääriä johtopäätöksiä.

## Fyysinen vaikuttaminen elektronisen sodankäynnin tukena

Edellä kuvattiin miten elektroninen vaikuttaminen voi tukea fyysistä asevaikutusta ja siltä suojautumista. Tuki toimii myös toisinpäin. Fyysisellä tulenkäytöllä voidaan tukea elektronista vaikuttamista tuhoamalla tai lamauttamalla sellaiset viesti- ja tutkajärjestelmät, joita ei saada häirittyä. Järjestelmän elektronisen sodankäynnin kestokyky voi riippua esimerkiksi isoista antennirakenteista, voimakkaasti suuntaavasta lanka-antennista tai teleskooppimastojen avulla aikaan saadusta suuresta antennikorkeudesta. Nämä rakennelmat edellyttävät yleensä jonkinlaista rakentamista ja sitovat järjestelmän toimimaan paikallaan. Mikäli fyysisellä tulenkäytöllä pakotetaan järjestelmä siirtymään usein, tai jopa toimimaan liikkeessä, se ei voi käyttää edellä mainittuja rakenteita elektroniseen suojautumiseen, vaan joutuu toimimaan esimerkiksi marssiantenneilla. Tällöin järjestelmä on huomattavasti helpommin häirittävissä. Fyysinen asevaikutus voi myös vaurioittaa järjestelmän antenneja, jolloin niiden säteilykuvio muuttuu ja suojausominaisuudet voivat heiketä. Mikäli vastustajan johtamisjärjestelmä lamautetaan elektronisella häirinnällä, sen on siirryttävä käyttämään varamenetelmiä, kuten käsimerkkejä ja lähettejä. Useiden varamenetelmien käyttöä kyetään häiritsemään epäsuoralla tulella.


**Kuva 38: Fyysinen asevaikutus tukee elektronista sodankäyntiä lamauttamalla vastustajan elektronisia järjestelmiä. Venäläisessä radioelektronisessa taistelussa fyysinen tuhoaminen on keskeisin vastustajan elektronisten järjestelmien lamauttamiskeino. Kuvassa venäläinen TOS-1-raketinheitinajoneuvo.** [J. Kosola]

Fyysisellä vaikuttamisella voidaan tukea myös omaa elektronista suojautumista paikantamalla vastustajan häirintäjärjestelmä oman elektronisen tuen joukolla sekä lamauttamalla se omalla tulenkäytöllä. Tulevaisuudessa vastustajan häirintäjärjestelmien tuhoamiseen voidaan käyttää tähän tarkoitukseen kehitettyjä ammuksia, joita voidaan käyttää myös vastustajan muiden lähetinten lamauttamiseen[46]. Näin fyysisellä vaikuttamisella voidaan tukea sekä omaa elektronista suojautumista että elektronista vaikuttamista.

## Psykologinen sodankäynti elektronisen sodankäynnin tukena

Psykologisen sodankäynnin keinoin voidaan tukea elektronista vaikuttamista esimerkiksi tuottamalla vastustajalle kuva niin ylivoimaisesta häirintäkyvystä, ettei tämä edes yritä kehittää vaihtoehtoisia suojautumismenetelmiä, tai antamalla vastustajan ymmärtää, että syy sen järjestelmien toimimattomuuteen on jossakin muualla kuin omassa elektronisessa vaikuttamisessa. Tällöin vastustaja kohdistaa omat suojautumis- ja vastatoimenpiteensä väärään suuntaan. Esimerkiksi Persianlahden sodissa ja Irakin lentokieltoalueiden valvonnassa samoin kuin Kosovon konfliktissa liittouma tuotti mielikuvia tutkan säteilyn välittömästi havaitsevista ja salaman nopeasti aktiivisiin tutkiin iskevistä koneista. On mahdollista, että tällä pyrittiin saamaan puolustaja pitämään ilmapuolustusjärjestelmänsä passiivisina. Jos osa

puolustajista ei uskalla aktivoida järjestelmäänsä, on loppujen järjestelmien häiritseminen ja tuhoaminen helpompaa. Psykologisen vaikuttamisen mahdollisesti paras käyttökohde tässä asiayhteydessä on luoda maaperä otolliseksi elektronisen vaikuttamisen tukemiseen tähtäävälle harhautusoperaatiolle.

Psykologisella suojautumisella voidaan suojautua vastustajan toteuttamilta edellä kuvatuilta toimilta tuottamalla tietoa vastustajan mahdollisesti käyttämistä psykologisista vaikuttamiskeinoista. Tuotetun tiedon on oltava todenmukaista, uskottavaa ja se on mahdollisuuksien mukaan viestittävä jo ennen vastustajan psykologista vaikuttamista.

# 4. ARVIO ELSO:N ELEMENTTIEN KEHITTYMISESTÄ TULEVAISUUDESSA

Luku perustuu kirjoittajien laatimaan puolustusvoimien sotatekniseen arvioon ja ennusteeseen vuonna 2004 laadittuun Elektronisen sodankäynnin kehittymistä käsittelevään lukuun.

## Elektroninen tuki

Elektronisen tuen järjestelmät kohtaavat jatkossa suuria ongelmia kohteiden teknisen kehittymisen vuoksi. Kohteiden havaitseminen, paikantaminen ja muu hyödyntäminen vaikeutuu oleellisesti viesti- ja tutkajärjestelmien signaalinkäsittelyominaisuuksien kehittymisen vuoksi. Signaalien parametreja vaihdellaan taajuuden, ajan ja paikan suhteen. Hajaspektritekniikat (suorahajotusmenetelmä), taajuushyppivät ja lyhyet purskelähetteet[m] yleistyvät edelleen viestijärjestelmissä, ja erilaiset LPI-tekniikat, lähetystaajuuden ja muiden parametrien nopea vaihtaminen, elektronisesti keilaavat antennit yms. tutkajärjestelmissä. Viestilähetteissä siirrytään yhä enemmän mikroaalto-alueelle, tutkalähetteissä millimetrialueelle ja optronisissa sovelluksissa infrapuna-alueelta ultraviolettialueelle, mitkä kaikki vaikuttavat elektronisen tuen järjestelmien vaatimuksiin.

Ongelman tuottaa myös viestijärjestelmien jatkuva digitalisoituminen sekä salauksessa ja muussa koodaamisessa vaadittavan prosessointitehon halpeneminen. Jatkossa yhä pienempi osa viestiliikenteestä siirtyy puheena tai muuten selkokielisenä lähetteenä. Viestiliikenteen havainnointi lähenee siten perinteistä tutkakohteiden elektronista tukea, jossa kohteita tarkastellaan niiden teknisten parametrien, ja lisäksi esim. liikenneanalyysin avulla. Signaalit ovat dataa ja purskelähetteitä, joiden tunnistamiseksi on kyettävä analysoimaan lähetteen kaistanleveys, taajuustarkkuus, modulointitapa, pulssin tai purskeen pituus ja muut vastaavat parametrit. Vaativimpia tehtäviä tulevat olemaan hajaspektritekniikalla kätkettyjen signaalien ja muun salatun datan havaitseminen ja tilastollinen selvittäminen. Tämä edellyttää signaalien laajakaistaista tallentamista ja tietokoneanalyysiä. Käyttöön tulevat yhä enenevässä määrin “tiedonlouhintatekniikat” (data mining), joilla relevantti tieto kaivetaan esiin suurista tietomassoista. On kuitenkin muistettava, että uuden tekniikan tulo laajamittaiseen käyttöön vie yleensä pitkän ajan ja esimerkiksi hajaspektritekniikkaa hyödyntävät viestivälineet yleistyvät vain kunkin maan rajallisten resurssien mahdollistamassa hankintatahdissa.

Koska modernien sotilaskäyttöön tarkoitettujen vaikeasti havaittavien ja häirittävien hajaspektrijärjestelmien käyttöönottoa hidastaa ja rajoittaa kyseisen teknologian kalleus, tullaan yhä kasvavassa määrin siirtymään kaupallisen teknologian (COTS,

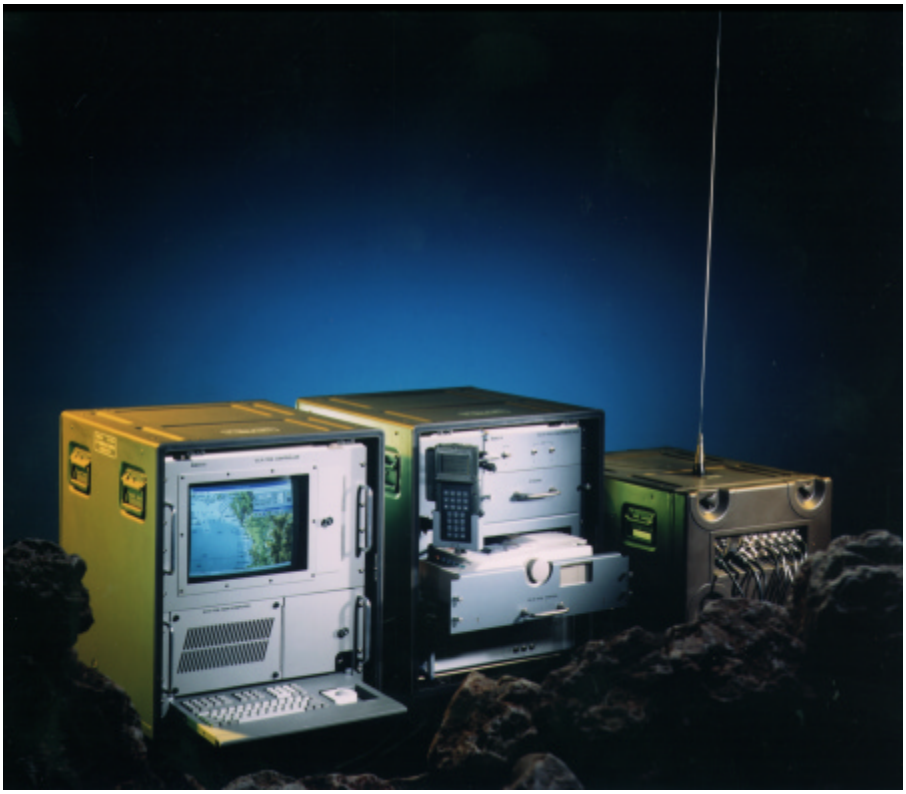
[m] Purkelähetteellä tarkoitetaan puolustusvoimissa ajallisesti lyhyttä datalähetettä.

Commercial Off The Shelf) käyttöön. Tämän kehityksen myötä tietoliikennesignaalien sieppaaminen ja tulkitseminen on tulossa entistä vaikeammaksi[47]. Tämä johtuu osin siitä, että nämä järjestelmät toimivat eri taajuusalueilla ja perustuvat erilaisiin teknisiin ratkaisuihin kuin perinteiset sotilasviestijärjestelmät, mutta myös siitä, että niissä otetaan nopeasti käyttöön tekniikan viimeisimpiä saavutuksia, kuten salaus, ja lisäksi siitä, että sotilasjärjestelmien lähetteet hukkuvat siviilijärjestelmien muodostamaan vilkkaaseen signaalitaustaan.

Toisaalta tekniikan yleinen digitalisoituminen tuo uusia mahdollisuuksia elektronisen tuen järjestelmille. Digitaalivastaanottimien yleistyminen ja digitaalisen signaalinkäsittelyn menetelmien ja prosessointitehon paraneminen tuo uusia mahdollisuuksia kehittyvien kohdejärjestelmien havainnointiin, kuten hajaspektrilähetteiden löytämiseen. Järjestelmät myös pienenevät kooltaan. Tämän kehityksen ääripäätä edustavat erikoisjoukoille kehitettävät erittäin pienikokoiset ja kevyet kannettavat tai taisteluvarustuksen osaksi puettavat miniatyyrihakusuuntimot. Niiden avulla taistelijat kykenevät havaitsemaan vastustajan käsiradiot, satelliitti- ja matkapuhelimet sekä johtamispaikkojen, panssarivaunujen yms. kenttäradiot ja muut radiolähettimet[48].

**Kuva 39: Israelilainen ELTA:n EL/K-7036-viestitiedustelujärjestelmä. HF-taajuusalueella lähetteiden tarkka suunnan mittaus vaatii useita HF-antennimastoja isolla antennikentällä. Korkeammat VHF- ja UHF-taajuudet voidaan mitata mastoon sijoitetuilla antenniryhmillä. Esimerkki laitetilassa olevista vastaanottimista on esitetty kuvassa 40.** [ELTA]

Elektronisen tuen järjestelmät kehittyvät yhä lähemmäksi strategisen signaalitiedustelun järjestelmiä, ja monet perinteisesti signaalitiedusteluun liittyvät tekniikat ja toiminnot, kuten yksittäisten lähettimien tunnistus (alustatunnistus, sormenjälkitunnistus) ja yhä tihenevän signaaliympäristön vaatimat analysointilaitteet ja älykkäät luokittelijat, ovat tulevaisuudessa tulossa myös taktiseen käyttöön.



**Kuva 40: Israelilaisen ELTA:n taktinen viestitiedustelujärjestelmä EL/K-7036, joka sisältää sekä haku- ja kuuntelu- että suuntimotoiminnot. Kuvassa järjestelmän käyttölaitteet, jotka voidaan liittää esimerkiksi kuvassa 39 esitettyihin antenneihin.** [ELTA]

Elektronisen tuen järjestelmät ovat viime vuosituhannella jakautuneet niiden kohdejärjestelmien mukaisesti viestijärjestelmien tiedusteluun, valvontaan ja kuunteluun (vrt. COMINT, Communications Intelligence) sekä viestintää sisältämättömien lähetteiden tiedusteluun, valvontaan ja analysointiin (vrt. ELINT, Electronic Intelligence). Kohdejärjestelmien tekninen kehitys tulee kuitenkin ennen pitkää sulauttamaan elektronisen tuen haarat yhdeksi kokonaisuudeksi. Viestijärjestelmät ovat digitaalisia ja salattuja, niiden signaalin modulointi ja koodaus muistuttaa koko ajan enemmän tutka- ja paikannusjärjestelmissä käytettävää koodausta, joten vastaavasti viesti-ELTU-järjestelmien on kyettävä samanlaiseen signaalinprosessointiin kuin tutka-ELTU-järjestelmienkin – sama pätee myös toisin päin. Kun lisäksi vielä viestijärjestelmien

käyttämä taajuusalue laajenee tutkataajuuksille ja toisaalta tutkien käyttämät taajuudet ulottuvat viestijärjestelmien perinteiselle kaistalle, tullaan siihen tilanteeseen, että ELTU-järjestelmien toimintataajuudet, antennirakenteet, vastaanottimet ja signaaliprosessointiyksiköt ovat samoja tai ainakin niin samankaltaisia, että järjestelmät sulautuvat yhteen elektronisen tuen kokonaisuudeksi. Vastaanotin-järjestelmät myös integroituvat signaalien monimutkaistumisen myötä, jolloin toisten vastaanotintyyppien heikkouksia täydennetään toisten hyvillä ominaisuuksilla.

Kasvava signaalitiheys, signaalirakenteiden kehittyminen yhä vaativammiksi, signaalien levittäytyminen yhä laajemmalle taajuusalueelle sekä teknisen analysoinnin korostuminen myös viestijärjestelmien tiedustelussa ja valvonnassa nostavat myös elektronisen tuen järjestelmien hintoja. Toisaalta olemme harvinaisen teknologisen murroksen kynnyksellä, jossa digitaalisista signaalinkäsittelyä ymmärtävät toimijat tunkeutuvat perinteisten valmistajien tontille. Tämä tuo uusia mahdollisuuksia myös kotimaiselle puolustusvälineteollisuudelle, mikäli tilaisuuteen ymmärretään tarttua.

**Kuva 41: Ewation/MRCM:n ELTU-järjestelmä MRD 4008. Kuvassa on järjestelmän vastaanotin-, prosessointi- ja käyttölaitteet. Toimiakseen järjestelmä tarvitsee lisäksi erilliset antennit, joita tässä kuvassa ei näy.** [ewation GmbH/MRCM]

Elektronisen tuen järjestelmien suorituskykyyn liittyy myös sensoreiden ja johtamis-järjestelmien verkottuminen. Havainnot tulee saada levitettyä nopeasti ja laajalle eri johtoportaissa. Tiedonsiirtomenetelmien ja esitysjärjestelmien kehittyminen tukee tätä

kehitystä, joskin perinteiset tietoturvallisuusvaateet voivat aiheuttaa tähän konflikteja. Tulevaisuutta ovat kuitenkin joka tasolla myös datafuusiojärjestelmät, joilla erityyppisten sensoreiden tietoja yhdistetään ja saadaan johtopäätöksille lisäarvoa.

Yleisenä elektronisen sodankäynnin kehitysvisiona on huomattava ohjelmistoradioiden kehittyminen: tulevaisuudessa samalla laitteella voi olla hyvinkin erilaisia viestiliikenne-, navigointi- ja jopa tutkasovelluksia, minkä lisäksi sitä voidaan käyttää älykkäästi elektroniseen tukeen ja vaikuttamiseen. Toisaalta ohjelmistoradiot asettavat suuria haasteita elektroniselle tuelle, sillä tietyn järjestelmän käyttäminen useaan eri tarkoitukseen vaikeuttaa vastapuolen elektronisen tuen johtopäätösten tekoa (esim. joukkojen tunnistamista lähettimien perusteella).

## Elektroninen vaikuttaminen

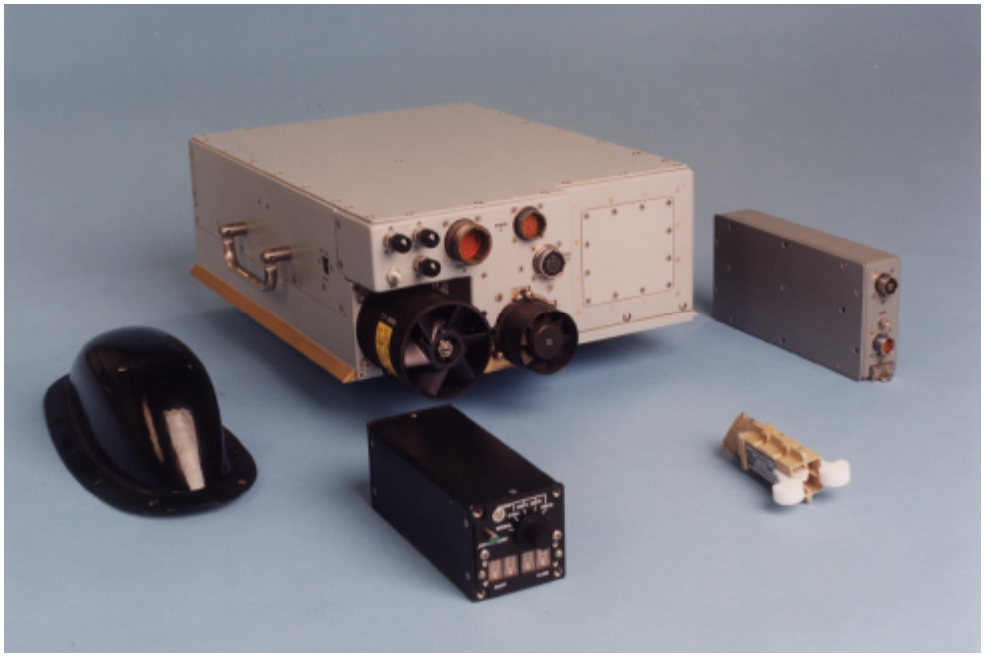
Elektroniseen harhauttamiseen ja vaikuttamiseen voidaan käyttää osin samoja järjestelmiä, joskin harhauttamisen saralla voidaan kekseliäillä yksinkertaisillakin järjestelmillä saada paljon aikaiseksi pienin kustannuksin. Harhautuksen merkitys korostuu tulevaisuuden elektronisella taistelukentällä, koska vastustajan sensori-järjestelmien kehittymisen myötä omaa toimintaa on hyvin vaikeaa pitää täysin salassa. Myös omat hyötylähetteet peittävä (maskaava) häirintä liittyy oman toiminnan salaamiseen. Joidenkin arvioiden mukaan elektronisesta harhautuksesta tulee tulevaisuudessa elektronisen vaikuttamisen keskeisin osa-alue.

Elektroninen häirintä kehittyy teknisesti jatkuvasti kilpajuoksussa kohdejärjestelmien häirinnänväistöominaisuuksien kanssa. Taajuushypytystä seuraavat viestihäirintä-lähettimet (following jammer) ja nopeasti kehittyviin digitaalisiin radiotaajuus-muisteihin (DRFM; Digital Radio Frequency Memory) perustuvat tutkahäirintä-lähettimet uhkaavat perinteisesti hyvin suojattuina pidettyjä järjestelmiä. Toisaalta uudet esim. älyantennitekniikkaan perustuvat suojautumismenetelmät tuovat häiritsijälle uutta päänvaivaa.

Vaikka järjestelmiä voidaan suojata häirinnältä monin erilaisin tekniikoin, häirintä on aina viime kädessä taistelua voimakkaimmasta lähetteestä. Lähelle tuotu häirintälähetin kykenee helpommin häiritsemään kohteensa, minkä vuoksi myös häirintälavettien kehitys etenee nopeaa tahtia kohti miehittämättömiä järjestelmiä. Tulevaisuudessa lennokit sekä massiivisesti käytettävät yksinkertaiset sirotettavat järjestelmät ovat potentiaalisia tiedustelu- ja häirintälavetteja, joskin niiden ongelmana on heikko sähkötehon tuotantokyky. Toisaalta vastaanottimen läheisyydessä toimittaessa tarvittava häirintäteho on pieni[49].

HF-alueella radiohäirinnän merkitys jäänee pieneksi, koska tehokkaan häirinnän järjestäminen on vaikeaa avaruusaallon ja suunta-antennien käytön vuoksi. VHF/UHF-alueilla radiohäirinnällä on tulevaisuudessa edelleenkin tärkeä merkitys. Tämän vuoksi elektroninen vaikuttaminen on integroitava muuhun tulenkäyttöön: fyysisellä tulen-käytöllä tai muita informaatiosodankäynnin keinoja käyttäen lamautetaan ne

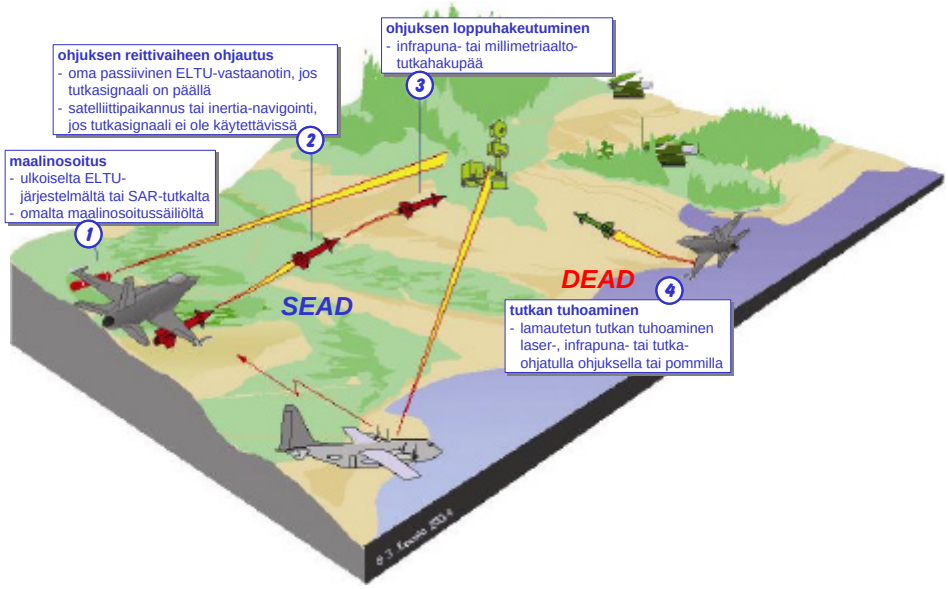
järjestelmät, joita ei voida häiritä, ja toisaalta elektronisella häirinnällä lamautetaan ne järjestelmät, joihin ei voida vaikuttaa muuten. Vain tällaisella kokonaisstrategialla voidaan saavuttaa tuloksia – muuten vastustajan käyttöön jää aina jokin varajärjestelmä, eikä häirinnästä sen paremmin kuin tulenkäytöstäkään saada kovin suurta hyötyä.



**Kuva 42: ELTA:n maa-ajoneuvoihin tai helikoptereihin asennettavissa oleva tutkahäirintäjärjestelmä. Antennit on sijoitettu aerodynaamisesti muotoiltujen radioaaltoja läpäisevien suojien sisälle (kuvassa vasemmalla). Muut järjestelmän laitteet on muotoiltu ilma-alusten ahtaisiin tiloihin ja käyttökonsoleihin sopiviksi.** [ELTA]

Elektroninen häirintä niveltyy usein tiiviisti yhteen vastustajan ilmapuolustuksen lamauttamisen tai tuhoamisen (SEAD/DEAD; Suppression/Destruction of Enemy Air Defenses) kanssa, mikä on nykyaikaisten sotien ensimmäisiä vaiheita. Ilmapuolustus-järjestelmää häiritään massiivisesti, mutta mahdollisuuksien ja tarpeen mukaan myös tuhotaan säteilyyn hakeutuvilla ohjuksilla (ARM; Anti Radiation Missile). SEAD-lavettien ja -kokonaisjärjestelmien kehitysprojektit ovat lähitulevaisuudessa ehkä suurimpia yksittäisiä elektronisen sodankäynnin hankkeita, erityisesti USA:ssa.

Häirintämenetelmät sivuavat myös psykologista sodankäyntiä. Tulevaisuuden sodissa kiinnitetään yhä enemmän huomiota ELSO-järjestelmien suuritehoisten lähettimien käyttöön informaatio-operaatioissa oman propagandan lähettämiseen ja vastustajan tiedotteiden estämiseen. Lavetteina toiminevat jatkossakin Compass Call -tyyppiset isot lentokoneet.




**Kuva 43: Esimerkki vastustajan ilmapuolustuksen lamauttamisesta (SEAD) ja sen jälkeisestä tuhoamisesta (DEAD). Tutkasäteilyyn hakeutuva ohjus voi saada maalinosoituksen ulkoisesta lähteestä (taistelunjohtokone, ELTU-kone, satelliitti) tai järjestelmän omasta maalinosoitussäiliöstä (targeting pod). Ohjus voi lentää reittivaiheen oman hakupäänsä ohjaamana tai maalina olevan tutkan sammutettua lähettimensä GPS- tai inertiaohjattuna. Terminaalivaiheessa ohjausmenetelmäksi voidaan vaihtaa passiivinen infrapuna tai aktiivinen millimetriaaltotutka.**

On syytä korostaa erikseen satelliittinavigointisignaalien häirintää. GPS on erittäin helposti häirittävä järjestelmä, ja sitä vastaan on myynnissä jopa kaupallisia häirintäjärjestelmiä. Satelliittinavigointijärjestelmällä tulee siten olla tulevaisuudessa aina varajärjestelmät. GPS-satelliitteihin ja -vastaanottimiin ollaan kehittämässä häirinnänväistöominaisuuksia, jotka perustuvat adaptiiviseen antennitekniikkaan sekä uuteen signaalirakenteeseen. On kuitenkin nähtävä, että häirintäjärjestelmät kykenevät myös tulevaisuudessa vaikeuttamaan GPS-järjestelmän toimintaa. Eurooppalaisessa Galileo-järjestelmässä ei ole erikseen huomioitu vihamielisen elektronisen häirinnän väistämistä.

Keskeinen tulevaisuuden kysymysmerkki on elektroniseen lamauttamiseen käytettävien radiotaajuisten aseiden yleistyminen. Erilaisia EMP- ja HPM-aseita tai niiden demonstraattoreita on jo olemassa, mutta niiden leviämisen laajuus ja laajamittaisen käyttöönoton aikataulu on avoin kysymys. Radiotaajuisten aseiden laaja käyttö muuttaisi oleellisesti järjestelmien suojausvaatimuksia ja koko nykyaikaisen sodan kuvaa. Monet sellaiset järjestelmät, joihin sodankäynti perustuu, olisivat täysin käyttökelvottomia. Erityisen haavoittuvia elektroniselle lamauttamiselle ovat elektronisen tuen järjestelmät sekä tutka- ja radiolinkkijärjestelmät.

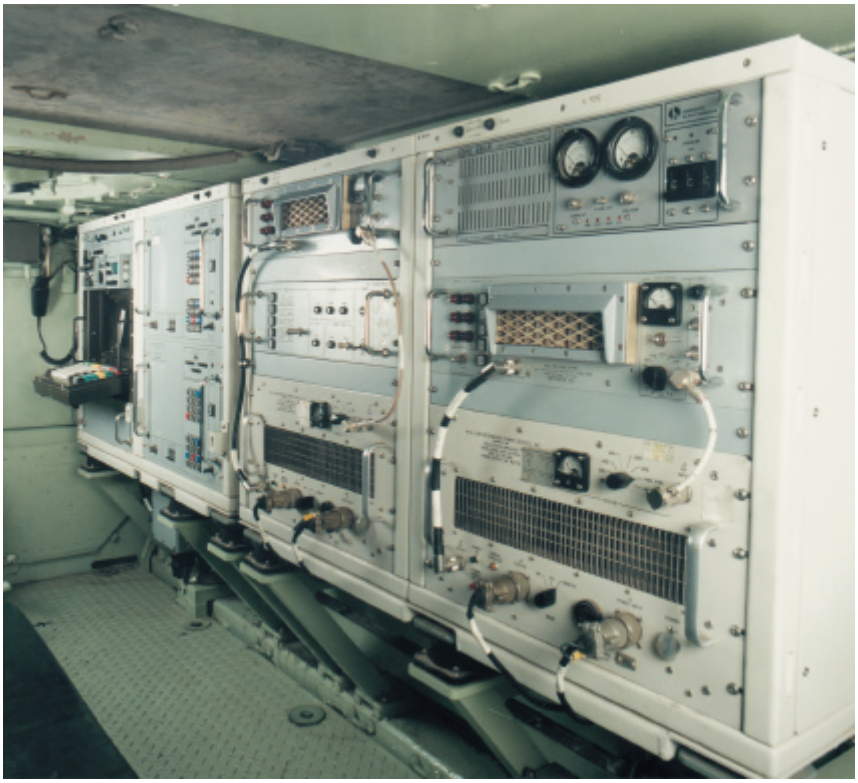
**Kuva 44: Israelilainen viestihäirintäjärjestelmä (COMJAM) asennettuna M-113 alustalle. Järjestelmä on saatettavissa nopeasti toimintakuntoon, sillä antennimastoja ei tarvitse harustaa maahan. Toisaalta harustuksen puuttumisen vuoksi antennikorkeus jää vaatimattomaksi.** [ELTA]

## Elektroninen suojautuminen

Elektroninen suojautuminen kehittyy sekä teknisenä haasteena että toimintakulttuurina. Elektronisilla suojausmenetelmillä pyritään vähentämään vastapuolen häirinnän ja harhautuksen vaikutusta sekä mahdollisuuksia siepata signaalejamme. Teknisesti näihin päämääriin pyritään mm. salaamalla viestien sisältö, lyhentämällä viestitysaikoja, hajauttamalla signaalit ajallisesti ja paikallisesti, suuntaamalla lähetteet sekä säätelemällä tehoja, kaistanleveyksiä ja modulaatioita.

Elektronisen suojautumisen tulee olla mukana kaikkien organisaatio- ja järjestelmätasojen operatiivisessa suunnittelussa. Oma toiminta tulee järjestää siten, että voidaan mahdollisimman tehokkaasti suojautua vastustajan tiedustelulta, elektroniselta tuelta ja elektroniselta vaikuttamiselta. Teknistä apua tähän tuo erilaisten radioaaltojen etenemistä analysoivien laskentamallien ja tietokoneohjelmien yleistyminen, sekä tilannekuvan levittäminen myös alemman tason joukoille tietoverkkojen myötä.

Elektronisen suojautumisen tulee olla oleellisena osana kaikkea tulevaisuuden harjoitustoimintaa. Sillä luodaan edellytykset sekä sodan ajan toiminnan osaamiselle, että estetään vastustajaa saamasta sodan ajan toiminnan kannalta kriittistä informaatiota rauhan aikaisista harjoituksista.



**Kuva 45: Sisäkuva viestihäirintäasemasta (Multi-Tasking COMJAM System).** [ELTA]

Passiivista elektronista suojautumista on kehitetty voimakkaasti viime vuosina, ja kehitys jatkuu tulevaisuudessa. Häivetekniikkaa kehitetään sekä tutkia että optronisia sensoreita vastaan, erityisesti materiaaliteknisin ja rakenteellisin keinoin. Tulevaisuudessa kaikkien lavettien suunnittelussa eräs keskeisimpiä suunnittelu-kriteereitä tulee olemaan alustan tutkapoikkipinta ja infrapunasormenjälki, olipa kyseessä maa-, meri- tai ilmalavetti.

Myös taajuushallinta ja laajempana käsitteenä emissioiden hallinta (EMCON) tulee kehittymään. Tähän vaikuttaa tietotekniikan ja -verkkojen kehittyminen ja sen mahdollistama reaaliaikainen taajuushallinta. Tämä mahdollistaisi myös hyvin älykkäät harhautustoimet, jos elektroninen vaikuttaminen, harhauttavat lähetteet ja omat hyötylähetteet saataisiin koordinoitua ovelasti.

Elektronisten järjestelmien yleinen kehittyminen tuo mahdollisuuksia elektroniseen suojautumiseen. Tällaisia mahdollisuuksia muodostavat mm. digitalisoitumisen ja signaalinkäsittelyn mahdollistama salauksen ja antennitekniikan kehittyminen. Antennitekniikassa joudutaan edelleenkin tekemään kompromisseja havaitsemisen todennäköisyyden, taajuusalueen, suuntimistarkkuuden ja kustannusten kesken. Elektronisesti keilaavat antennit yleistyvät lähitulevaisuudessa kaikissa sovelluksissa kaukovalvontatutkista aseiden hakupäihin. Niiden seuraava kehitys askel on ns. tila-aika- (Space-Time Coding) ja MIMO-prosessointi (Multiple Input – Multiple Output). Tällaisen järjestelmän häirintä onnistuu teoriassa vain sirottamalla sen läheisyyteen lukuisia häirintälähettimiä, sillä järjestelmä kykenee poistamaan useista suunnista tulevan häirintäsignaalin ja hyödyntämään kaiken eri suunnista ja eri aikaan saamansa signaali-informaation.

**Kuva 46: Esimerkki HF-taajuusalueen häirintäjärjestelmästä. HF-taajuuksilla aallonpituus on useita metrejä, joten tarvittavat antennirakenteet vaativat paljon tilaa. Tämä sekä HF-lähetteiden pitkä kantama ja siten kolmansille osapuolille aiheutetut häiriöt tekevät HF-häirinnästä melko ongelmallista ja siten VHF- ja UHF-taajuuksien häirintää harvinaisempaa.** [ewation GmbH/MRCM]

Erityisinä elektronisen suojautumisen tekniikoina kehittyvät taajuushypintä ja suora-hajotushajaspektritekniikka, jotka yleistyvät tulevaisuudessa kaikilla viestiliikenteen tasoilla. Viestiverkot muuttuvat tulevaisuudessa monipalveluverkoiksi, joilla on useita vaihtoehtoisia väyliä käytössään, joten esimerkiksi häirinnän vaikutusta voidaan väistää.

Adaptiiviset älyantennit mahdollistavat hyötysignaalin suuntaamisen haluttuun suuntaan ja häirintäsignaalin vaimentamisen. Elektronista suojautumista tarjoaa tavallaan myös satelliittiviestiliikenteen kehittyminen ja yleistyminen suuntaavine antenneineen, joskin satelliittiviestiliikenteen tiedustelu ja häirintä voi olla järjestelmästä riippuen hyvinkin helppoa.

Tutkatekniikan puolella kehittyvät erilaiset LPI-tekniikat, kuten tutkan signaali-parametrien nopea hypytys, kantoaalto- (continuous wave, CW) ja jopa satunnais-aaltomuototutka, sekä elektronisesti keilaavat antennit. Monipaikkatutkaa ja sen käytännön toteuttamista tullaan tutkimaan edelleen. Näitä tekniikoita tukee yleinen signaaliprosessoinnin kehittyminen. Kehityksessä on havaittavissa selvä jako joko hyvin kalliisiin ja monimutkaisiin ratkaisuihin (esim. täysin elektronisesti keilaavat tutkat) tai halpoihin ja yksikertaisiin ratkaisuihin (esim. taajuushypytys), joita sovelletaan jo käytössä oleviin tutkiin.

Omasuojajärjestelmät kehittyvät kaikissa lavettiympäristöissä. Ilma-alusten omasuojajärjestelmien peruskokoonpanona toimii edelleen korkealla toimivissa aluksissa (hävittäjät yms.) tutkavaroitin ja matalalla toimivissa (helikopterit yms.) ohjusvaroitin, sekä kaikissa alustyypeissä yleensä silpun- ja soihdunheitin. Nämä kaikki elementit kehittyvät nopeasti: tutkavaroittimien prosessointi kehittyy lähemmäksi automaattisia elektronisen tuen järjestelmiä. Ohjusvaroitin voi olla aktiivinen tutka, mutta yleisemmin IP- tai UV-sensori, tulevaisuudessa molempien taajuusalueiden kuvaava ja ohjusta seuraava sensori. Silput ja soihdut ovat vanhaa perustekniikkaa, mutta myös niissä kehitystä tapahtuu erityisesti spektrin, palo-ominaisuuksien ja liikkuvuuden suhteen siten, että heitteen herätteen ominaisuudet ja liikevektori vastaavat suojattavan kohteen ominaisuuksia sillä tarkkuudella, jolle ohjukset kehittyvät. Heitteiden yhdeksi vielä ratkaistavaksi ongelmaksi jää kuitenkin kuvaavan hakupään häirintä tai harhauttaminen etäisyydeltä, jolta ohjus on jo kyennyt muodostamaan maalista kuvan hakupäähänsä.

Etenkin korkealla liikkuvissa ilma-aluksissa myös aktiivisen omasuojahäirinnän merkitys korostuu. Tämä tekniikka kehittyy toisaalta vastaavasti kuin elektroninen vaikuttaminen, mutta tulevaisuudessa korostuu aluksen perässä hinattavien häirintälähettimien merkitys. Omasuojahäirintä lähestyvää ohjusta vastaan on siinä määrin vaativa ongelma, että mahdollisuuksia parantaa huomattavasti häirintä- tai harhautuslähettimen sijoittaminen kauemmaksi aluksesta, jolloin ei haittaa vaikka ohjus havaitsisi häirinnän ja hakeutuisi häirintälähettimeen. Myös alukseen sijoitettu tutkahäirintä kehittyy mm. erilaisten DRFM-tekniikkaan ja esim. aaltorintamien vaiheominaisuuksiin perustuvien häirintämenetelmien (cross-eye) myötä.

Infrapunaohjuksia vastaan kehitetään erilaisia suunnattuun häirintävaikutukseen perustuvia menetelmiä (DIRCM), jotka etenkin tulevaisuudessa perustuvat ohjuksen hakupään häirintään, sokaisuun tai sen elektroniikan tuhoamiseen suunnatulla lasersäteellä. Tällainen järjestelmä vaatii kehittyneen ohjusvaroittimen ja seuranta-järjestelmän. Yleisen terrorismiuhkan vuoksi nimenomaan halvat ja yksinkertaiset olalta laukaistavat IP-ohjukset vievät lähitulevaisuuden omasuojakehitystä eteenpäin: arvokkaat vihamielisessä ympäristössä matalalla toimivat tai uhka-alueelle laskeutuvat

ja nousevat helikopterit sekä kuljetuskoneet vaativat jatkossa kehittyneitä infrapuna-häirintämenetelmiä. Myös kaupallisten matkustajakoneiden suojaamisesta on ollut paljon keskustelua ja tietyt lentoyhtiöt ovat ottaneet tai tulevaisuudessa ottavat järjestelmiä käyttöön pahimmilla uhka-alueilla. Lasersäteen seuraajaohjusten yleistyminen lisää myös laservaroitinten käyttöä ilma-aluksissa. Tällaiselta ohjukselta suojautuminen on kuitenkin erittäin vaikeata ja edellyttää käytännössä laserkujan muodostavan asejärjestelmälavetin seurantasensorin (tutka, infrapuna tai näkyvän valon kamera) sokaisua tai harhauttamista.

Laivojen omasuojajärjestelmät kehittyvät myös jatkuvasti. Suuremman koon, sähköntuotantokyvyn yms. vuoksi järjestelmät voivat olla oleellisesti suurempia ja monipuolisempia kuin ilma-aluksissa, minkä lisäksi myös suojattavan aluksen arvo on ilma-aluksia suurempi ja pakenemiskyky heikompi. Laivojen uhkavaroitinjärjestelmät toimivat kaikilla ELSO:n taajuusalueilla ja kehittyvät suorituskyvyltään lähelle jopa tiedusteluvastaanottimia ja -prosessoreita, joskin pääpaino on mahdollisimman suuressa havaitsemisen todennäköisyydessä ja nopeassa vasteessa. Etenkin laser-ohjattuja pommeja ja meritorjuntaohjuksia vastaan tarkoitetut laservaroittimet ja uhkaa vastaavat vastatoimenpidelaitteistot yleistyvät ja kehittyvät.

Laivojen omasuojahäirintälähettimet kehittyvät myös, joskin meritorjuntaohjuksiin investoidaan ilmataistelu- ja ilmatorjuntaohjuksia enemmän häirinnänväistö-ominaisuuksia ohjuksen suuremman koon ja arvokkaamman maalin ansiosta. Tämän vuoksi omasuojahäirintä itse lavetilta voi olla jopa vaarallista, joskin tietyt lupaavat häirintämenetelmät (esim. cross-eye) kehittyvät jatkuvasti. Kehitys on kuitenkin erityisen voimakasta erilaisten passiivisten ja aktiivisten heitteiden saralla. Tutkien häirintään käytettyjen perinteisten silppujen ja suojasavujen edelleen kehittämisen lisäksi kehitetään erilaisia suojasumuja sekä kaasutäytteisiä soppiheijastimia. Heitteet vastaavat asejärjestelmien kehitykseen luomalla suojaa yhä laajemmalla taajuusalueella (ns. multispektraaliset heitteet). Lisäksi kehitetään hinattavia sekä miehittämättömiä aluksia (UAV/USV) sekä rakettipoijulla ammuttavia aktiivisia häirintä- ja harhautus-lähettimiä ja infrapunaharhamaaleja. Perinteisten tutka- ja IP-uhkien lisäksi tulevaisuudessa pyritään laivoilla harhauttamaan laservalaisuun perustuvia ohjuksia Tähän kehitykseen vaikuttaa maailmalla yleinen toimintaympäristön siirtyminen avovesiltä lähemmäksi rannikkoa.

Panssarivaunujen ja muiden ajoneuvojen omasuojaa parannetaan tutka- ja laser-varoittimin sekä niihin liitetyin savutus- ja sumutusjärjestelmin. Myös passiivisia infrapuna- ja ultraviolettivaroittimia kehitetään. Tällä hetkellä ja lähitulevaisuudessa tilanne on se, että teknisiä ratkaisuja lavettien omasuojan kehittämiseen on olemassa, mutta järjestelmiä ei juurikaan ole varusteltu. Hakeutuvien ja ohjattavien ammusten voimakas lisääntyminen kuitenkin pakottaa varustamaan tärkeimmät lavetit (taisteluvaunut, komentoajoneuvot ja muut johtamisjärjestelmän ajoneuvot, ilmatorjuntavaunut jne.) jonkinlaisella omasuojajärjestelmällä. Se, mitä komponentteja (laser-, tutka-, infrapuna- tai ultraviolettivaroitin, visuaali-, infrapuna- tai tutkaheite, muutoin levitettävä suojaverho tai vasta-ammus tms. suoja) lopulta valitaan, riippuu uhkan kehittymisestä. Uhkan kehitys puolestaan riippuu paitsi teknisestä kehityksestä, myös valittavasta operaatioalueesta. Perinteisellä taistelukentällä uhkana ovat kaukaa

toimivat älykkäät aseet, kun taas kriisinhallintaoperaatiossa ensisijaisena uhkana ovat lähellä ja mahdollisesti siviiliväestön keskuudesta käytettävät matalateknologiset aseet, kuten singot.

Maalavettien suojauksessa perusongelmana on aina se, että järjestelmät ovat kalliita lavetin hintaan suhteutettuna ja panssarintorjuntaohjusten tms. aseiden häirintäjärjestelmät ovat erityisen vaikeita ja kalliita toteuttaa. Etenkin erilaisin häive- ja harhautusmenetelmin lavetteja voidaan suojata hyvinkin tehokkaasti, mikäli toiminnan suunnittelu on tarpeeksi älykästä. Potentiaalisina tulevaisuuden järjestelminä kehittyvät DIRCM-laitteet, pitkälti samalta pohjalta ja osin jopa samoissa projekteissa kuin ilmaaluksille. Panssariajoneuvojen omasuoja voi luonnollisesti perustua myös perinteisesti lähestyvien ohjusten fyysiseen tuhoamiseen esim. sirpaleammuksin tai heittein.

## ELSO-tukitoiminta

ELSO-tukitoiminnan kehittymiseen liittyy elektronisen sodankäynnin järjestelmien tekniikan kehittyminen, jonka myötä ELSO-järjestelmät ja strategisen signaalitiedustelun järjestelmät ovat teknisesti lähentyneet toisiaan. Sensorijärjestelmien kehittymisen myötä myös elektronisen sodankäynnin yksiköt tarvitsevat yksityiskohtaisia signaalikirjastoja ja muita tietokantoja; samoin myös häirintämenetelmien tulee olla erittäin tarkoin suunniteltuja.

Tietoverkkojen ja tietokantojen kehittyminen auttaa ELSO-tukitoiminnan reaaliaikaisuustarpeen saavuttamisessa. Tavoitteena on saada mahdollisimman lyhyet vasteet uusimmista havainnoista koko käsittelyketjun läpi aina ELSO-joukkojen päivitettyihin tietokantoihin asti.

# 5. TIETOTURVALLISUUS ELEKTRONISESSA SODANKÄYNNISSÄ

## Salassapito on suorituskyvyn edellytys

Luvussa kuvataan erilaisia sellaisia huomioon otettavia seikkoja, jotka liittyvät elektronisen sodankäynnin yhteydessä esiin tulevien asioiden luokitteluun eri tiedon luottamuksellisuusluokkiin. Kirjassa ei käsitellä sitä, miten tietoturvaluokiteltua tietoa käsitellään, tallennetaan tai siirretään, sillä siitä on oma ohjeistuksensa valtion-hallinnossa ja puolustusvoimissa.

Elektroninen sodankäynti on sodankäynnin osa-alue, jonka rooli taisteluiden, operaatioiden tai jopa koko sotatoimen lopputuloksessa on suhteellisen vähän tunnettu. Tämä johtunee paljolti siitä, että elektronisen sodankäynnin suurimmat saavutukset ovat perustuneet siihen, ettei toinen osapuoli ole osannut ennakoida vastapuolen uutta teknologiaa, teknistä sovellusta tai yllättävää toimintatapaa tai siitä, ettei se ole älynnyt korjata toimintatapaansa ELSO-sietoisemmaksi, koska ei osannut yhdistää kärsimiään tappioita ja kokemiaan vaikeuksia toisen osapuolen elektroniseen sodankäyntiin. Elektronisen sodankäynnin rooli ja suorituskyky on siten nimenomaisesti haluttu pitää mahdollisimman pienen piirin tiedossa. Jopa elektroniseen sodankäyntiin liittyvä perustekniikka on usein pidetty salaisena.

Elektronisen sodankäynnin järjestelmän hyödyntäminen edellyttää sen teknisen toteutuksen, toiminnallisten innovaatioiden ja tarkan suorituskyvyn salassa pitämistä. Toisaalta taas elektronisen sodankäynnin kehittäminen samoin kuin puolustushaarojen taktiikan ja operaatiotaidon kehittäminen kärsii turhasta salailusta. Salassa pidettävien ja julkisten asioiden määrittäminen ei siten ole helppoa. Seuraavassa on kuitenkin pyritty kuvaamaan mitkä asiat tulee pitää ehdottoman luottamuksellisina ja missä kohdin luottamuksellisuus ei ole välttämätöntä. On kuitenkin syytä korostaa, että jokaisen tiedon luokittelu tulee tehdä tapauskohtaisesti.

***Jos et tunne aihetta riittävästi, tai jos et ole varma tiedon harmitto-muudesta, tieto on pidettävä lähtökohtaisesti turvaluokiteltuna, jos kyseessä on elektroniseen sodankäyntiin liittyvä asia.***

Salassa pidettäviä asioita ovat esimerkiksi

- Yksityiskohtainen, todellisiin joukkoihin ja järjestelmiin sidottu uhkakuva. Se antaa kuvan tiedustelujärjestelmämme suorituskyvystä sekä viitteitä järjestelmien ja joukkojen käyttöajatuksista ja suorituskykyvaatimuksista.
- Puolustusvoimien suorituskykyvaatimukset ja puolustushaarojen osuudet niiden täyttämisessä.

- Elektronisen sodankäynnin järjestelmän tekninen ja operatiivinen suorituskyky sekä käyttöperiaatteet. Luonnonlakien asettamat yleiset raja-arvot suorituskyvylle, kuten radiohorisontin olemassaolo ja etäisyys tietyllä antennikorkeudella, eivät kuitenkaan ole salassa pidettäviä.
- Elektronisen taistelukentän kuvaus parametritietoineen.
- Elektronisen sodankäynnin joukkojen koko, määrä ja organisoiminen sekä niiden kaluston ja henkilöstön määrä ja laatu.
- Tiedustelu-, valvonta-, johtamis- ja asejärjestelmille asetettavat yksityiskohtaiset tekniset ja toiminnalliset vaatimukset, joilla varmistetaan niiden toimivuus elektronisella taistelukentällä.
- Arviot keskeisten puolustusjärjestelmien toimivuudesta elektronisella taistelukentällä ja tähän liittyvät testit, raportit yms. tieto. Yksittäisen järjestelmän osalta esimerkiksi hankintaprosessiin liittyen tietosuojauksen tarve voidaan arvioida ja toteutus suunnitella tapauskohtaisesti.
- ELTU-järjestelmien signaalikirjastot ja ELVA-järjestelmien häirintäkirjastot.
- Tiedustelu-, valvonta-, johtamis- ja asejärjestelmien elektronisen suojautumisen (hypintä-, limitys-, salaus- jne.) sotamoodit, algoritmit ja niiden avainten muodostaminen sekä taajuuksien jakaminen näiden käyttöön.
- Sellaiset elektronisen sodankäynnin tekniset innovaatiot, jotka eivät ole yleisessä tiedossa, tai yleisesti tiedossa olevan teknisen innovaation normaalista poikkeava ja yllättävä soveltaminen.
- Teknillisen tutkimus- ja kehittämistoiminnan kokonaistavoitteet, tutkimushankkeiden tila ja saavutukset.
- Elektronisen tuen tutka- ja viestijärjestelmistä keräämät tiedot.
- Järjestelmien yleiset radiotekniset parametrit, kuten lähetysteho, antennivahvistus[n], hypintänopeus, pyyhkäisynopeus ja käytetty taajuuskaista. Toisaalta monet näistä ovat keskeisen tärkeitä järjestelmien elektronisen suojautumisen kannalta, toisaalta ne ovat usein pääteltävissä yleisistä teknologian ja tekniikan asettamista reunaehdoista ja tarkastelemalla järjestelmää esimerkiksi asenäyttelyissä.
- ELSO-järjestelmien sovellusohjelmistojen ominaisuudet, koska ne määrittävät miten järjestelmä toimii sekä miten se kykenee hyödyntämään sensoreiden keräämää tietoa.

[n] Huolimatta siitä, että antennin koosta voidaan arvioida sen vahvistus kun tiedetään järjestelmän karkea toimintataajuus, tarkan vahvistuksen kertominen julkisuudessa mahdollistaa tämän tiedon ja antennin koon perusteella antennissa käytetyn valaisufunktion arvioimisen. Tämä puolestaan johtaa järjestelmän elektronisen suojatason kannalta kriittisen ominaisuuden, sivukeilatason, paljastumiseen.

Harkinnan mukaan salassa pidettäviä asioita voivat olla esimerkiksi:

- Geneerinen uhkakuva, joka kuvaa elektronisen sodankäynnin kohteet ja käytetyt menetelmät yleisellä tasolla, muttei sisällä viittauksia todellisiin kohteisiin tai joukkoihin eikä yksityiskohtia järjestelmien ominaisuuksista tai joukkojen käytöstä. Kuten liitteestä 6 käy ilmi, geneerinen uhkakuva ja vastustaja voi olla myös julkinen, vaikka se sisältäisikin kuvauksia joukoista ja järjestelmistä.
- Elektronisen taistelukentän kuvaus ilman tarkkoja parametreja, joista voitaisiin laskea mille tasolle puolustusjärjestelmämme on suunniteltu. Kuvaus voidaan myös luokitella siten, että kokonaisuus on tiukemmin luokiteltu kuin siitä otetut otteet.
- Käytössä olevat elektronisen sodankäynnin laitteet ja järjestelmät sekä niiden nimitykset ja tyypit. Joissakin maissa jopa järjestelmien nimet on pyritty pitämään salaisina vastapuolen tiedonhankinnan estämiseksi, kun taas joissakin toisissa maissa julkistetaan jopa järjestelmiin hankittavien laitteiden merkit ja mallit ajatellen, että laitteet joka tapauksessa ovat kaupallisia tuotteita.
- Valtakunnallinen koulutusjärjestelmä, jolla muodostetaan yhteinen käsite-maailma ja yhtenäinen perusta osaamiselle ja toimintatavoille.
- Elektronisen sodankäynnin palveluksessa olevan henkilöstön määrä, laatu ja henkilöiden identiteetti. Länsimaisissa avoimissa yhteiskunnissa tällaisen tiedon pitäminen salaisena myös käytännössä voi olla hankalaa, mutta toisaalta käsitys henkilöstön määrästä ja laadusta kertoo suoraan puolustusjärjestelmän elektronisen sodankäynnin suorituskyvystä. Henkilöiden identiteetin paljastaminen puolestaan mahdollistaa rauhan ja kriisin eskaloitumisen aikana tiedustelun kohdistamisen ja sodan aikana fyysisen ja psykologisen vaikuttamisen kohdistamisen mahdollisiin avainhenkilöihin.
- Elektronisen sodankäynnin organisointi ja vastuiden määrittäminen yleisellä tasolla.

## Salailu heikentää saavutettavissa olevaa suorituskykyä

Haittana kaikesta elektroniseen sodankäyntiin liittyvästä salamyhkäisyydestä on luonnollisesti se, ettei oman elektronisen sodankäynnin joukkojen ja järjestelmien roolia osata arvostaa, taktiset johtajat eivät osaa käyttää käytössään olevia ELSO-joukkoja, vastustajan elektronisen sodankäynnin suorituskykyä ei tunneta, ja sen vaikutusta omaan operaatioon ei osata arvioida. Suurimpana uhkana puolustusvoimien kokonaissuorituskyvyn kannalta on kuitenkin se, ettei elektronisen sodankäynnin järjestelmien hankintaan ja joukkojen varustamiseen osata kohdentaa riittäviä resursseja, jos yleisjohtajat eivät tunne elektronisen sodankäynnin tuomia mahdollisuuksia ja uhkia.

***Liika salailu johtaa ennen pitkää siihen, että tieto, joka vastustajalla joka tapauksessa jo on, ei kulje omassa organisaatiossa sitä tarvitseville.***

Julkisia asioita ovat *yleensä*

- Käsitteet ja määritelmät.
- Elektronisen sodankäynnin mukanaan tuomat uhat sekä elektronisen sodankäynnin rooli taistelussa ja yleiset käyttömahdollisuudet operaatioissa.
- Yleiset toimintaperiaatteet.
- Elektronisen häirinnän vaikutus tutka- ja viestijärjestelmiin ja häirintäjärjestelmien yleinen suorituskyky tarkasteltuna yleisten teknisten reunaehtojen ja yleisesti tiedossa olevien menetelmien tasolla. Häirintäjärjestelmät perustuvat kaikkialla suurin piirtein samanlaiseen teknologiaan, joten tietynkokoiselle lavetille voidaan tila-, paino-, tehontarve-, jäähdytys- yms. rajoitusten vuoksi asentaa tietyn lähetysteholuokan häirintäjärjestelmä. Säteilyn eteneminen lähettimeltä kohteelle samoin kuin häirintäjärjestelmien vaikutus voidaan laskea tietokoneella yksinkertaisilla taulukkolaskenta-ohjelmilla tai yleisessä käytössä olevilla karttapohjaan perustuvilla laskentaohjelmilla sekä arvioida yksinkertaisilla peukalosäännöillä. Näiden yleisesti pääteltävissä olevien tekijöiden perusteella voidaan todeta, miltä karkealta etäisyydeltä eri tavoin suoritettu häirintä kykenee vaikuttamaan järjestelmiin.
- Yleisohjeet siitä, *mitä* asioita elektronista sodankäynnistä tulee huomioida taistelun suunnittelussa ja toteuttamisessa. Se, *miten* nämä asiat missäkin tilanteessa huomioidaan, on lähes aina salassa pidettävää tietoa.
- Elektronisen tuen yleinen suorituskyky. Elektronisen tuen kantama voidaan arvioida lähetystehon, antennin ja laskettavissa olevan etenemisvaimennuksen sekä eri tyyppisten elektronisen tuen vastaanotinten tunnettujen herkkyyksien avulla vastaavasti kuin häirinnän tapauksessa.
- Suurin osa elektronisen sodankäynnin tekniikoista, jotka itse asiassa ovat ”normaalin” tutka-, radio-, antenni-, tieto- ja tiedonsiirtotekniikan, puolijohde- ja tehoelektroniikan sekä digitaalisen signaalinkäsittelyn soveltamista sotilaalliseen käyttöön.

Edellä on kuvattu yleensä salassa pidettäviä asiakategorioita sekä harkinnan mukaan salassa pidettäviä tietoja, jotka ainakin Suomessa on yleensä tietoturvaluokiteltu salassa pidettäviksi. Kuvauksella ei ole pyritty osoittamaan sitä, mitkä asiat ovat tai minkä pitäisi olla salassa pidettäviä tai julkisia Suomessa, vaan asian käsittelyn tarkoituksena on herättää lukijaa ajattelemaan itse, mitä perusteita tai seurannaisvaikutuksia erilaisen tiedon salassa pitämisellä tai julkisuuteen avaamisella voi olla.

## Tietoturvaluokituksen lähtökohdat

Asioiden tietoturvaluokittelussa on muistettava, että tietoja voidaan luokitella useilla eri perusteilla. Tieto voi itsessään olla salainen, tai jokin siihen suoraan tai välillisesti liittyvä seikka voi johtaa tarpeeseen pitää sinänsä julkinen tieto salassa. Tietoturvaluokituksessa perusteena voi olla esimerkiksi jokin seuraavista:

- Tiedon itsensä pitäminen salassa: vastustaja ei kykene arvioimaan järjestelmiemme ja joukkojemme suorituskykyä eikä optimoimaan vasta-toimiaan niitä vastaan.
- Sen salaaminen, mitä jostakin vastustajaan liittyvästä asiasta tiedetään: vastustaja ei osaa muuttaa toimintatapojaan, koska ei arvaa meidän tuntevan jotakin tämän heikkoutta.
- Sen salaaminen, mitä ei tiedetä: vastustaja ei kykene päättelemään aukkoja tiedustelussamme, ei kykene hyödyntämään osaamispuutteitamme omassa operaatioissaan ja joutuu varautumaan siihenkin vaihtoehtoon, että tunnemme jonkin heikkouden tämän järjestelmässä.
- Tiedon lähteen tai syntyprosessin salaaminen, vaikkei tieto itsessään olisikaan salainen. Tällä suojataan omaa tiedustelu-, valvonta- ja johtamisjärjestelmää sekä päätöksentekoa vastustajan tiedustelulta ja vaikuttamiselta.
- Vastustajan tiedustelun suuntaamisen vaikeuttaminen: jo järjestelmän nimi tai tyyppi voi herättää vastustajan tiedustelun mielenkiinnon ja auttaa kohdistamaan tiedustelu tärkeisiin kohteisiin sekä asettamaan tarkkoja tiedustelukysymyksiä[50].
- Vastustajan tiedustelun pakottaminen toimimaan laajalla rintamalla: kun vastustajalle ei tarjota valmiina kaikkea julkista tietoa, se joutuu kohdentamaan resurssejaan ja käyttämään aikaa perustietojen keräämiseen, jolloin sillä on vähemmän mahdollisuuksia kerätä tietoja meille tärkeiltä alueilta.

# 6. ELEKTRONISEN SODANKÄYNNIN HUOMIOIMINEN KEHITTÄMISOHJELMISSA

Elektronisen sodankäynnin yhtenä ongelmana on usein se, että vaikka ymmärrettäisiin sen antamat mahdollisuudet omalle toiminnalle, on kovin vaikeata mieltää, että myös vastustaja käyttää näitä samoja menetelmiä ja tekniikoita sekä meitä vastaan että omaksi suojakseen. Vaikka esimerkiksi elektroninen tuki antaa tarkan kuvan vastustajan toiminnasta ja sijainnista sekä tietoja sen taktiikasta ja tekniikasta, ei ELSO-alan ulkopuolella usein ymmärretä, että vastaavasti vastustajan käytössä olevat elektronisen tuen järjestelmät antavat samat tiedot omista järjestelmistämme ja joukoistamme. Olennaista onkin siis tarkastella samanaikaisesti sekä omia että vastustajan mahdollisuuksia. Vastustajan tehokkaimpien vastatoimenpiteiden kohteena ovat luonnollisesti omat tehokkaimmat järjestelmämme, joten vastustajan osaamisen ja tekniikan aliarviointi on tuhon ensimmäinen askel. Amerikkalaisten sotakokemusten mukaan ***kolmannes järjestelmän määrittelyyn ja kehittämiseen käytettävistä resurssista tulisikin kohdentaa vastustajan toimintamahdollisuuksien arvioimiseen ja näihin vastatoimenpiteiden kehittämiseen***.

Seuraavassa käsitellään tiivistetysti ja yleisellä tasolla sitä, miten elektronisen sodankäynnin mukanaan tuomat uhkat ja mahdollisuudet tulee ottaa huomioon kehittämisohjelmissa.

Puolustusvoimien suorituskykyä kehitetään valtakunnallisilla ja puolustushaara-kohtaisilla kehittämisohjelmilla. Kehittämisohjelma on laaja kokonaisuus erilaisia hankkeita, joilla luodaan kehittämisohjelman perusteena oleva suorituskyky. Suoritus-kykyvaatimukset puolustushaaroille sekä puolustusjärjestelmän osajärjestelmille saadaan puolustusvoimien strategiselta suunnittelulta[51], joka myös kuvaa kokonais-järjestelmän operatiivisen konseptin eli sen missä ympäristössä ja miten puolustus-järjestelmän kokonaisuutta ja osajärjestelmiä suunnitellaan käytettävän[52].

Puolustusjärjestelmän suorituskykyvaatimusten täyttämiseksi etsitään puolustus-voimien hankeohjausmallin mukaisesti erilaisia vaihtoehtoisia tai toisiaan täydentäviä konsepteja. Näille määritettävissä suorituskykyvaatimuksissa tulee kuvata[53]:

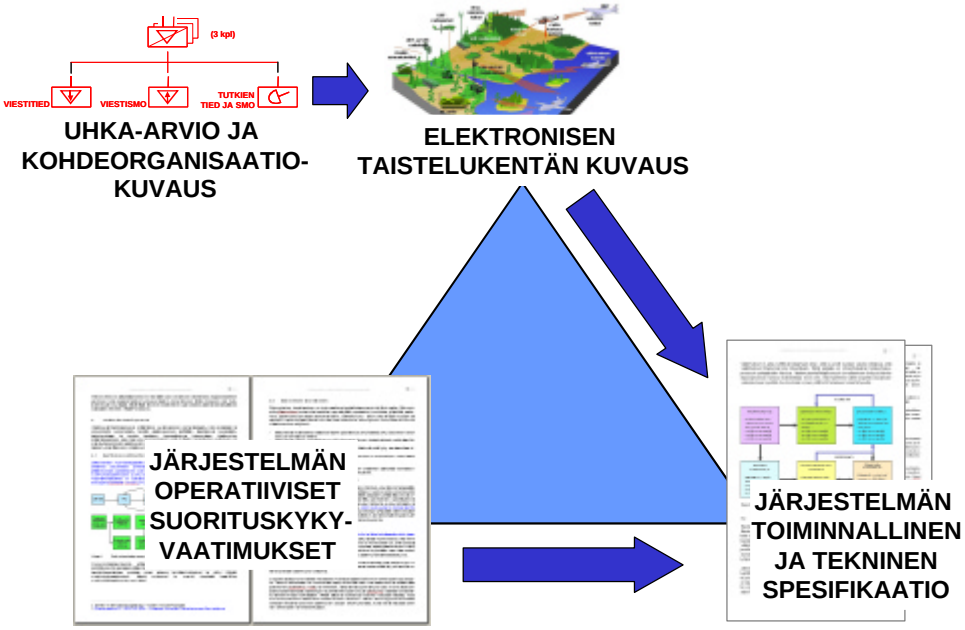
- Järjestelmältä edellytetty suorituskyky, kuten tyypillinen tai minimi hyväksyt-tävä kantama, yhteysväli tms. seikka.
- Järjestelmään kohdistuva uhka, jonka alaisena edellä kuvattu suorituskyky tulee saavuttaa.

Suorituskykyä tulee tarkastella nimenomaan vastustajan mahdollisesti toimeenpanemia vastatoimenpiteitä vasten, siis elektronisen taistelukentän olosuhteissa. Olennaista on esimerkiksi viestijärjestelmän kantama häirinnän alaisena todellisessa taistelu-tilanteessa, ei järjestelmän tekninen suorituskyky rauhan aikaisessa harjoituskäytössä.

Järjestelmän suorituskyky koostuu seuraavista kolmesta tekijästä:

- materiaali: varsinainen järjestelmä, tukeutumisjärjestelmä…
- henkilöstö: lähtötaso, koulutus, kokemus, osaaminen, motivaatio…
- toiminta: doktriini, ohjesääntö, opas, käyttöohje…

Näiden kaikkien osa-alueiden on oltava kunnossa. Kehittämisohjelmien valmistelussa päähuomio tulee kuitenkin kiinnittää materiaalin elektronisen sodankäynnin kestoon. Tässä yhteydessä on kyettävä myös kuvaamaan ne skenaariot, joissa suorituskyky-vaatimukset pätevät. Esimerkiksi rauhan ajan harjoitustoiminnassa häirinnänsietoa tärkeämpää voi olla vastustajan signaalitiedustelun vaikeuttaminen, kun taas kriisi-aikana toimintakyky häirinnän alla voi olla tiedustelulta suojautumista tärkeämpää.




**Kuva 47: Järjestelmän kyky toimia elektronisella taistelukentällä varmistetaan sisällyttämällä elektronisen suojautumisen asettamat toiminnalliset ja tekniset vaatimukset järjestelmän spesifikaatioihin. Ne saadaan järjestelmän suorituskyky-vaatimusten ja käyttöolosuhteiden mukaisen uhka-arvion perusteella.**

Järjestelmään kohdistuva ELSO-uhka käsittää

- Vastustajan tiedustelu-, valvonta- ja maalinosoitusjärjestelmät, erityisesti signaalitiedustelun ja elektronisen tuen avaruudessa, ilmassa ja pinnassa toimivat sensorit.
- Vastustajan pinnassa ja ennen kaikkea ilmassa toimivat häirintäjärjestelmät.
- Vastustajan elektronisen lamauttamisen järjestelmät.

Mikäli tarkasteltavana on asejärjestelmä, uhkaan on sisällytettävä myös vastustajan omasuojajärjestelmät.

Uhkasta tulee kyetä kuvaamaan ainakin se, missä tilanteissa vastustaja pyrkii vaikuttamaan mihinkin järjestelmämme osaan sekä millä välineillä ja miltä etäisyydeltä vaikutus toteutetaan. Tämän karkean järjestelmään sen aiotussa käyttöympäristössä ja käyttötilanteessa kohdistuvan uhkan kuvauksen perusteella elektronisen sodankäynnin asiantuntijat kykenevät:

- laatimaan tarkemman järjestelmäspesifisen uhkakuvauksen
- laatimaan uhkakuvauksen ja operatiivisten suorituskykyvaatimusten perusteella järjestelmän teknisen ja toiminnallisen spesifikaation

On huomattava, että vaikka elektronisen sodankäynnin tekniikat ja näihin liittyvät järjestelmävaatimukset ovat elektronisen sodankäynnin upseereiden ja insinöörien spesifistä ammattitaitoa, kehittämisohjelman suorituskykyvaatimuksiin kuuluvien operatiivisten vaatimusten, operatiivisen konseptin ja kehitettävää suorituskykyä vastaan kohdistuvan uhkan karkea määrittely on nimenomaan kehittämisohjelman suorituskyvyn luomisen ohjaajan tehtävä – siis yleisosaamista.

# 7. ELEKTRONINEN SODANKÄYNTI SOTAHISTORIASSA

Edellä on jo käsitelty elektronisen sodankäynnin roolia joissakin historiallisissa tilanteissa. Näitä esimerkkejä ei tässä enää toisteta, vaan käsittelyn tarkoituksena on tuoda lisää taustatietämystä aihepiiriin. Tässä yhteydessä elektronisen sodankäynnin historiaan ei pyritä saamaan kattavaa eri aikakaudet ja sotien eri osapuolet läpikäyvää näkemystä, vaan ainoastaan tuoda esiin esimerkkejä ELSO:n merkityksestä toiminnan eri osa-alueiden kannalta.

Seuraavassa on poimittu teemoittain joitakin sotahistorian enemmän tai vähemmän tunnettuja tapahtumia tai seikkoja, joissa elektronisella sodankäynnillä oli sodan, operaation tai taistelun lopputuloksen kannalta keskeinen merkitys. Elektronisen sodankäynninkin historiaan perehdyttäessä on kuitenkin aina muistettava suhtautua kriittisesti lähteisiin. ELSO:n historia on pitkälti toisen maailmansodan voittajien kirjoittamaa. Vaikka liittoutuneiden elektroninen sodankäynti, erityisesti strateginen signaalitiedustelu ja operatiivis-taktinen elektroninen tuki ja häirintä, olivat ratkaisevassa asemassa toisen maailmansodan lopputuloksen kannalta, myös akselivaltojen ja Suomen elektroninen sodankäynti toi oman panoksensa taisteluun, vaikka niistä onkin vähemmän painettua materiaalia saatavilla. Toinen lähdekritiikin yhteydessä muistettava seikka on se, että elektronisen sodankäynnin perus-edellytyksenä on sen yllättävyys vastustajalle. Tämän vuoksi ELSO:n roolia ei yleensä juurikaan mainita sotien aikana tai edes muutaman kymmenen vuoden kuluessa sodan jälkeen. Toisaalta toimimattomia ratkaisuja saatetaan kovastikin kehua, jotta muiden huomio saadaan suunnattua pois asioiden todellisesta laidasta.

## Elektronisen tuen antamat tiedot ovat oikein käytettyinä avain voittoon

Ensimmäisessä maailmansodassa saksalaisten voitto venäläisistä Tannenbergissä perustui siihen, että heidän radiotiedustelunsa kykeni selvittämään venäläisten kahden armeijan ryhmityksen ja etenemisaikataulun. Ratkaisevin kuitenkin oli mm. radioliikennettä seuraamalla saatu tieto venäläisten armeijoiden komentajien äärimmäisen heikoista keskinäisistä väleistä. Saksalaiset kykenivät laskemaan sen varaan, että toinen komentaja ei tulisi toisen avuksi. Tämä mahdollisti sen, että saksalaiset kykenivät lyömään ensin toisen ja sitten toisen armeijan ennen kuin venäläisvoimat ehtivät yhtyä.

Toisessa maailmansodassa Midwayn meritaistelu käänsi Tyynenmeren sodan kulun lopullisesti amerikkalaisten hyväksi. Amiraali Nimiz tiesi USA:n signaalitiedustelun perusteella japanilaisten hyökkäyksestä Midwaylle hyökkäyksen ajankohdan sekä hyökkäyksessä käytettävät joukot. Nimitz kykeni näillä tiedoilla ryhmittämään joukkonsa oikeaan aikaan japanilaisten todennäköisintä toimintavaihtoehtoa vastaan.

Näin amerikkalaiset kykenivät välttämään japanilaisten joukkonsa suojaksi ryhmittämät tiedusteluosat sekä osasivat jättää japanilaisten operatiivisen harhautuksen omaan arvoonsa[54]. Operaation lopputuloksena Japanin laivasto menetti neljä lentotukialustaan. Menetysten vuoksi Japani joutui luopumaan hyökkäyksestä Midwaylle ja aloite Tyynenmeren sodassa siirtyi lopullisesti amerikkalaisille.

Toisessa maailmansodassa Saksalaisen taistelulaiva Scharnhorstin tuhon varmisti brittien elektroninen sodankäyntikyky ja saksalaisten tappion sinetöi heidän heikompi ELSO-osaamisensa. Brittien signaalitiedustelu paljasti saksalaisten operaatio-kokonaisuuden. Signaalitiedustelun antamien tietojen avulla Royal Navy kykeni viemään paikalle oikeaan aikaan riittävät voimat. Briteillä oli siis selkeä käsitys saksalaisten voimista ja niiden käytön suuntautumisesta ja ajoituksesta. Saksalaisella laivasto-osastolla taas ei ollut käsitystä alueella olevista voimakkaista brittien laivasto-osastoista[o]. Erot strategisen elektronisen tiedustelun kyvyssä asettivat laivastojen komentajat selkeästi eri asemaan: britit tiesivät saksalaisten operaation ajoituksen, kohteen ja käytettävät voimat, kun taas saksalaisilla ei ollut aavistustakaan alueella toimivista Royal Navyn voimista. Tämän operatiivisen edun lisäksi briteillä oli selkeä taktinen etu: HMS Duke of York oli varustettu moderneilla elektronisilla järjestelmillä: nimittäin ilma- ja pintavaroitustutkalla, kahdella erilaisella tulenjohtotutkalla, kahdella erilaisella omatunnistusjärjestelmällä sekä ELTU-järjestelmällä, jota saksalaiset erityisesti varoivat. Pintatutkat sekä tulenjohtotutkat mahdollistivat maalien löytämisen ja tulen johtamisen myös ilman visuaalista kontaktia. Olennaisin hyöty briteille tuli kuitenkin ELTU-järjestelmästä. Scharnhorst koetti välttää brittien takaa-ajoa pitämällä omaa tutkaa sammutettuna, jotteivät britit kykenisi paikantamaan sitä ELTU-järjestelmillään. Koska saksalaiset eivät olleet varustaneet Scharnhorstia ELTU-järjestelmällä, oli lopputuloksena se, että britit kykenivät seuraamaan tutkillaan saksalaista taistelulaivaa, joka puolestaan ei uskaltanut itse käyttää tutkaansa. Lopputulos ei olisi muuttunut, vaikka Scharnhorst olisikin käyttänyt tutkaansa, sillä tällöin britit olisivat voineet sammuttaa omansa ja seurata saksalaista alusta omilla ELTU-järjestelmillään huomattavasti kauempaa kuin Scharnhorst olisi kyennyt aktiivisella tutkalla havaitsemaan brittien risteilijät ja taistelulaivat[55].

## Suhteellinen etu vastustajaan nähden voi olla olemassa vain lyhyen ajan

Uuden aseen tai menetelmän käyttöönoton tulisi tapahtua mahdollisimman nopeasti ja laajamittaisesti, yllättäen sekä ennen kaikkea oikeassa sodan vaiheessa, sillä vastustaja kehittää nopeasti vastatoimenpiteitä, joilla toisen osapuolen saavuttama suhteellinen etu kiistetään. Esimerkiksi toisessa maailmansodassa saksalaisten kehittämä ilmasta

[o] Vaikka Luftwaffen partiokoneet olivat havainneet brittien voimat, tieto ei koskaan päätynyt saksalaiselle laivasto-osastolle, sillä puolustushaarojen viestijärjestelmien hankintaa ei Saksassa koordinoitu, eikä Kriegsmarine siten kyennyt ottamaan vastaan Luftwaffen lentokoneiden radioviestejä.

laukaistava radio-ohjattu HS-293-meritorjuntaohjus[p] mahdollisti jopa taistelulaivan kokoisen maalin upottamisen. Saksalaisten käytettyä asetta vähitellen ja sinänsä toisarvoisten maalien tuhoamiseen kykenivät britit elektronisen tuen antamien tietojen perusteella kehittämään aseen ja sitä ohjaavan lentokoneen välisen komentolinkin toiminnan estävän häirintäjärjestelmän. Tämä riisti saksalaisten suhteellisen edun ja palautti tilanteen ennalleen: ilmahyökkäykset oli jälleen tehtävä syöksy-, vaaka- tai torpedopommituksin alusten ilmatorjunnan kantaman sisäpuolelta.

## Olennaista on tuntea vastapuolen järjestelmät

Vastustajan aliarviointi on aina ollut kohtalokasta sodankäynnissä, mutta erityisesti elektronisessa sodankäynnissä, joka kulminoituu laadulliseen ja pitkälti älylliseen ylivoimaan. Esimerkiksi saksalaiset, jotka eivät toisessa maailmansodassa itse kyenneet valmistamaan korkeilla taajuusalueilla toimivia tutkajärjestelmiä, eivät uskoneet brittienkään tähän pystyvän. Siten Kriegsmarinen sukellusveneet oli varustettu vain matalan taajuusalueen tutkavaroittimilla. Ne eivät kuitenkaan paljastaneet korkeammilla taajuuksilla toimivia merivalvonta- ja sukellusveneentorjuntakoneiden tutkia. Tappioiden kasvaessa saksalaisten kannalta hälyttäviin mittoihin nämä, omien infrapunatutkimustensa ja oman tutkaosaamisensa ohjaamina, keskittivät voimansa sukellusveneiden lämpösuojauksen sekä heille tutulla taajuusalueella toimivien tutkasäteilyä absorboivien materiaalien kehittämiseen. Tästä ei tuossa tilanteessa luonnollisestikaan ollut mitään hyötyä. Kun saksalaiset lisäksi aliarvioivat brittien signaalitiedustelun suorituskyvyn ja kyvyn purkaa salausmenetelmiä, heidän tappionsa oli väistämätön.

## Myös omien järjestelmien tunteminen on tärkeätä

Omien järjestelmien toisilleen aiheuttamat häiriöt on tunnettava. Esimerkiksi HMS Sheffieldin uppoamiseen Falklandin sodassa vaikutti olennaisesti laivan järjestelmien käyttö siten, että sen oma viestijärjestelmä esti aluksen elektronisen sodankäynnin järjestelmän toiminnan. HMS Sheffieldin ELTU-järjestelmä ei kyennyt havaitsemaan argentiinalaista Super Etendard-rynnäkkökonetta ja sen laukaisemaa Exocet-ohjusta, koska aluksen kapteeni keskusteli 8-12 GHz kaistalla toimivalla satelliittiyhteydellä puolustusministeriön kanssa. Voimakas läheltä tuleva lähete sokaisi aluksen ELTU-järjestelmän näillä taajuuksilla, minkä vuoksi se ei kyennyt havaitsemaan 9,5 GHz alueella toimivan Exocetin tutkahakupäätä.

[p] Itse asiassa HS-293 oli rakettiavusteinen radio-ohjattu liitopommi.

## Salassapito on usein edellytys toiminnan onnistumiselle

Ilmataistelua Englannin yllä 1940 helpotti se, että britit kykenivät selvittämään signaalitiedustelulla saksalaisten Lorenz-, Knickebein-, X-Gerät- ja Y-Gerät-radiosuunnistusjärjestelmät jo niiden kokeiluvaiheessa. Häirintäjärjestelmät modifioitiin pikaisesti muun muassa sairaalalaitteista ja TV-lähettimistä. Tämä mahdollisti sen, että englantilaisilla oli häirintäjärjestelmä valmiina käytössä jopa jo ennen kuin Luftwaffe oli saanut oman suunnistusjärjestelmänsä laajaan operatiiviseen käyttöön.

Eri maiden signaalitiedustelun ja salausmenetelmien purkamisen merkitys taisteluiden ja sotien kulkuun on paljastettu toisen maailmansodan osalta vasta 1970-luvulta alkaen. Salassapidolla on luonnollisesti haluttu estää mahdollisia vastustajia korjaamasta toimintaansa siten, etteivät nämä menetelmät enää toimi.

## Liika salassapito saattaa estää toiminnan onnistumisen

Elektronisen sodankäynnin keinovalikoiman käyttöä voi rajoittaa se, että keinot tehoavat parhaiten mikäli ne tulevat vastustajalle yllätyksenä, tai ovat vielä niin uusia, ettei se ole ehtinyt sopeuttaa toimintaansa tai ei ole ehtinyt kehittää teknisiä vastatoimenpiteitä.

Esimerkiksi britit eivät pitkään uskaltaneet käyttää jo vuonna 1937 keksimäänsä silppua, jota he kutsuivat peitenimellä Window, sillä he pelkäsivät saksalaisten saavan näin tietoonsa tehokkaan keinon brittien ilmapuolustustutkien lamauttamiseksi. Tämä oli perusteltua niin kauan kuin saksalaisten pommitusten torjunta Britannian yllä oli tärkeämpää kuin brittien omien pommitusten suojaaminen Saksassa. Sotatilanteen muututtua silppua käytettiin lopulta 24.7.1943 tehdyn massiivisen 791 lentokoneen pommitusoperaation suojaamiseksi. Tällöin pommikoneista pudotetulla alumiinisilpulla estettiin saksalaisten Würzburg-tutkien ohjaaman ilmapuolustuksen toiminta. Yllättäen toteutettu operaatio oli menestys: vain 12 lentokonetta menetettiin, mikä edusti 1,6% lentokoneista, kun aiemmin menetykset olivat olleet 6% luokkaa. Elektronisen suojautumisen käyttö pelasti siis noin 40 lentokonetta ja 240 miehistön jäsentä pelkästään tässä yhdessä operaatiossa.

Amerikkalaiset seurasivat brittien silppututkimuksia ja kehittelivät sitä teknisesti kyeten saavuttamaan saman suorituskyvyn kapeammalla ja siten keveämmällä rakenteella. Amerikkalaisten suurin saavutus oli kuitenkin silpun, jota he kutsuivat termillä chaff, massatuotannon kehittäminen. Tätä varten valjastettiin myös alumiinipakkauksia valmistavia siviiliyrityksiä sotatarviketuotantoon. Ongelmaksi tuli kuitenkin se, että silppu on leikattava puolen aallonpituuden mittaiseksi uhkajärjestelmään nähden. Uhkajärjestelmä ja sen tekniset parametrit, kuten aallonpituus, ovat kuitenkin strategisen tiedustelun tuottamina salaista tietoa. Kummallinen tilanne syntyi, kun viranomaiset toisaalta halusivat yritysten tuottavan oikean mittaista silppua, mutteivät toisaalta suostuneet kertomaan mikä tuo oikea mitta olisi![56]

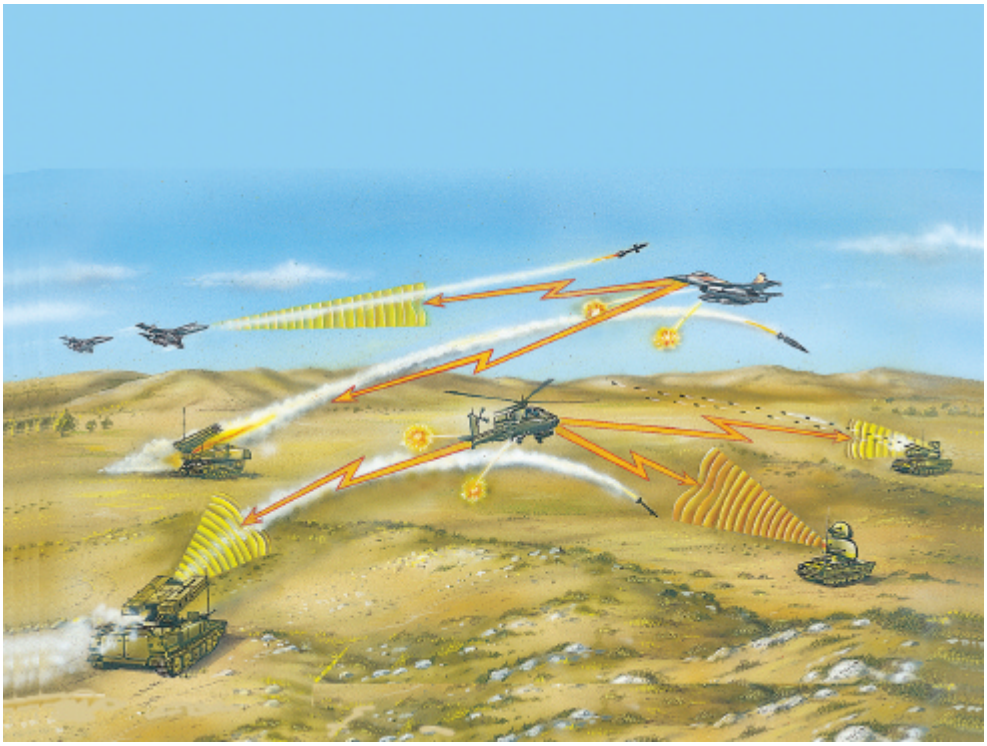
## Harhautus tukee tehokkaasti elektronista suojautumista

Yksi varsin kuvaava esimerkki harhauttamisesta elektronisen suojautumisen keinona löytyy brittiläisen toisen maailmansodan aikaisen tiedemiehen R. V. Jonesin kirjasta *Most Secret War*[57]. Britit olivat kehittämässä strategisiin pommituskoneisiinsa ”Gee”-tarkkuuspommitusjärjestelmää, jota tarvittiin pommikoneiden ohjaamiseen maalin ylle yöpommituksissa, joissa muut paikantamis- ja navigointimenetelmät olivat osoittautuneet liian epätarkoiksi tai epäluotettaviksi. Järjestelmä koostui Englannissa sijaitsevista radiolähettimistä ja muutamaan pommikoneeseen asennettavista vastaanottimista. Järjestelmää kokeiltiin lukuisia kertoja Saksan yllä, jolloin yksi paikantamislaitteella varustettu kone putosi. Britit pelkäsivät saksalaisten havaitsevan uuden laitteen, purkavan sen ja kehittävän häirintälaitteistot ennen kuin britit ehtisivät saada järjestelmää operatiiviseen käyttöön. Näinhän oli käynyt pari vuotta aikaisemmin, jolloin vastaavasti saksalaisten koekäyttämällä tarkkuuspommitus-järjestelmällä varustettu kone saatiin ammuttua alas ja britit onnistuivat kehittämään ja ottamaan operatiiviseen käyttöön häirintäjärjestelmät ennen kuin saksalaiset saivat tarkkuuspommitusjärjestelmänsä operatiiviseen käyttöön. Britit arvioivat tarvitsevansa vielä seitsemän kuukautta saadakseen oman pommitusjärjestelmänsä kehitettyä ja valmistettua. Harhautus toteutettiin seuraavasti: Ensiksi laitteen nimi ja tuotekilvet vaihdettiin. Alkuperäinen nimi R3000, joka indikoi pulssivastaanotinta, vaihdettiin tietoliikennejärjestelmissä käytettäväksi tyyppinimeksi TR1335, joka kuvaa lähetin-vastaanotinta (paikannusvastaanotinhan ei lähettänyt mitään). Nimen vaihtaminen oli tärkeätä siksikin, että pommikoneiden laitekehikot, liittimet ja johdotukset oli varustettu tehtailla jo kauan ennen kuin itse laite olisi valmis. Tyhjistä kehikoista valmiine kaapelointeineen saksalaiset joka tapauksissa arvaisivat jotakin uutta olevan tulossa. Harhauttavan tyyppinimen käyttäminen johtaisi heidät uskomaan, että britit ovat varustamassa pommikoneensa jollakin uudella radiojärjestelmällä. Gee-järjestelmän lähettimet Englannin Kanaalin rannikolla naamioitiin tavallisiksi tutka-järjestelmiksi lisäämällä ylimääräisiä mastoja ja valeantenneja. Koska saksalaisten signaalitiedustelu kuitenkin havaitsisi uuden tyyppiset signaalit, päätettiin heitä harhauttaa myös signaalirakenteen osalta poistamalla pulssien tarkka synkronointi. Harhautusta täydennettiin luomalla kaapattujen saksalaisagenttien avulla kuva siitä, että britit olisivat itse asiassa kopioimassa saksalaisten radiopaikannusjärjestelmää omaan käyttöönsä. Tätä tietolähdettä täydennettiin vielä todella lähettämällä tällaisia signaaleita pommitushyökkäysten aikana. Harhautuksen onnistumista kuvaa se, että ensimmäiset saksalaisten yritykset häiritä brittien tarkkuuspaikannusta tulivat vasta viisi kuukautta Gee-järjestelmän laajamittaisen operatiivisen käyttöönoton jälkeen.

## ELSO on tehokkain joukon suorituskykyä lisäävä tekijä

Kirjan johtopäätösluvussa kuvataan miten Israelin ilmavoimien suorituskyky moninkertaistettiin elektronisen sodankäynnin järjestelmien ja menetelmien käytöllä,

jolloin Bekaan laaksossa 1982 saavutettiin pudotussuhde 80:1 syyrialaisia vastaan[q]. Muita esimerkkejä löytyy esimerkiksi Vietnamin sodasta, jossa tausta- ja omasuojahäirintälentokoneet, ilmapuolustuksen lamauttamiseen käytettävät F-4G Phantom -hävittäjistä modifioidut ja HARM-ohjuksin varustetut EF-4G Wild Weasel SEAD-koneet sekä lentokoneiden varustaminen omasuojajärjestelmillä vähensivät vietnamilaisten ilmatorjunnan tehokkuuden seitsemänteen osaan: kun aiemmin oli tarvittu kymmenen ohjusta yhteen pudotukseen, tarvittiin nyt 70 ohjuslaukaisua pudottamaan yksi amerikkalainen lentokone. Joidenkin tietojen mukaan vuonna 1972 tarvittiin 150 SA-2 -ohjusta pudottamaan yksi amerikkalaiskone. Ottamatta kantaa todellisiin pudotussuhteisiin, voidaan todeta, että ilmatorjuntaohjusten tehottomuus oli niin hälyttävä ongelma, että venäläiset ryhtyivät kehittämään häirinnänväistö-menetelmiä, joiden käyttöönoton jälkeen pudotussuhde taas kohosi.



**Kuva 48: Vastustajan hallussa olevan alueen päällä ja lähellä lentäminen edellyttää lentokoneiden ja helikoptereiden varustamista omasuojajärjestelmillä.** [ELTA]

Kolmantena esimerkkinä elektronisen sodankäynnin keskeisestä vaikutuksesta joukon ja asejärjestelmän suorituskykyyn voidaan mainita vuoden 1973 ns. Jom Kippur -sota, jossa syyrialaiset ampuivat kuutisenkymmentä Styx-meritorjuntaohjusta osumatta yhteenkään israelilaiseen alukseen. Vastaavasti tekniseltä suorituskyvyltään

[q] Eri lähteissä on esitetty israelilaisten pudotusmääräksi 70 – 92 konetta heidän omien tappioidensa ollessa 0 – 1 kpl.

heikommat, mutta elektronisesti suojatummat, israelilaisten Gabriel-ohjukset upottivat 17 alusta.

USA:n johtaman liittouman pienet lentokonetappiot 1991 Persianlahden sodassa johtuivat muun muassa seuraavien tekijöiden yhteisvaikutuksena[58]:

1. Lentotehtävien suunnittelussa hyödynnettiin elektronisen tiedustelun vastustajan ilmapuolustusjärjestelmästä tuottamia tietoja. Tällä pystyttiin välttämään pahimmat uhka-alueet ja hyödyntämään irakilaisten ilmapuolustusjärjestelmään synnytettyjä aukkoja.
2. Muun muassa elektronisen tiedustelun avulla maalitettu vastustajan ilmapuolustusjärjestelmä lamautettiin häirinnällä ja tuhottiin fyysisesti.
3. Ilmapuolustusjärjestelmän lamauttamiseen käytettiin myös tutkasäteilyyn hakeutuvia ohjuksia.
4. Irakilaisten ilmatorjuntajärjestelmien tulen osuvuus pienennettiin häviävän pieneksi lentokoneiden elektronisen suojautumisen keinoin. Lentokoneet varustettiin uhkaa vastaavin varoittimin ja tutkien sekä ohjusten sokaisuun ja harhauttamiseen kykenevin häirintälaitteistoin. Niiden parametrointi irakilaisten tutka- ja ohjusuhkaa vastaan perustui mm. signaalitiedustelulla ja elektronisella tuella kerättyihin tietoihin irakilaisten ilmapuolustusjärjestelmästä.
5. Ilmaoperaatioita tuettiin tausta- ja saattohäirinnällä, joka pienensi irakilaisten ilmapuolustusjärjestelmän valvonta- ja seurantatutkien kantamaa niin paljon, että järjestelmään syntyi liittouman koneiden lähes vapaan liikkumisen mahdollistavia aukkoja. Häirintätehtävien suunnittelu ja häirintäjärjestelmien ohjelmointi perustui elektronisen tuen vastustajan joukoista ja järjestelmistä keräämiin tietoihin.
6. Irakilaisten ilmapuolustuksen harhauttamiseksi sekä houkuttelemiseksi toimimaan liittouman koneita vastaan käytettiin erilaisia lentäviä valemaaleja. Näillä ilmasta laukaistavilla harhalähettimin varustetuilla liidokeilla (TALD, Tactical Air-Launched Decoy) voitiin tarpeen mukaan kyllästää irakilaisten ilmapuolustus, peittää oma operaatio, houkutella irakilaiset tuhlaamaan ohjuksiaan harhakohteisiin tai pitää irakilaisten tutkat aktiivisina oman tutkasäteilyyn hakeutuvien ohjusten hyökkäyksen toteuttamiseksi.
7. Edellä kuvatuilla menetelmillä hajotettiin irakilaisten johtamisjärjestelmä ja estettiin tilannekuvan muodostaminen. Toisaalta liittouma ylläpiti lähes reaaliaikaista tilannekuvaa ilmaan sijoitetuilla sensoreilla. Lentävien kohteiden tutkavalvontaan käytettiin AWACS-järjestelmää (Airborne Warning And Control System), joka sisältää sekä kaukovalvontaan kykenevän ilmavalvontatutkan että hävittäjien johtamiseen kykenevän taistelunjohtojärjestelmän. Paikallaan olevat ja liikkuvat pintakohteet paikannettiin JSTARS-lentokoneella (Joint Surveillance and Target Acquisition Radar System), jonka SAR- ja GMTI-tutkat kykenivät muodostamaan metriluokan resoluutiolla lähes reaaliaikaista kuvaa syvältä taistelualueelta. Lisäksi elektronisen

tiedustelun RC-135 Rivet Joint -koneet muodostivat elektronista tilannekuvaa ja tunnistivat muilla sensoreilla havaittuja maaleja sekä valvoivat sähkömagneettisen spektrin käyttöä.

8. Liittouma kykeni estämään oman toimintansa ja operaatioajatuksen paljastumisen irakilaisten tiedustelulle ylläpitämällä operaatioturvallisuutta mm. suojaamalla omat viestiyhteytensä sekä harhauttamalla ja häiritsemällä irakilaisten tiedustelujärjestelmää.

**Kuva 49: Saksalaisia Hummel-häirintäpanssariajoneuvoja aavikolla** [ewation GmbH/MRCM]

Vaikka Yhdysvaltain johtaman liittouman ylivoima selittää sodan väistämättömän lopputuloksen, voidaan kuitenkin katsoa elektronisen sodankäynnin osaltaan selittävän sodan erittäin lyhyen keston ja liittouman äärimmäisen pienet tappiot.

## ELSO:n käyttöperiaatteita ja kokemuksia Venäjän sodissa tshetsheenejä vastaan

Seuraavassa käsitellään signaalitiedustelun ja elektronisen sodankäynnin toteutusta ja siitä saatuja kokemuksia Tshetshenian ensimmäisen sodan (1994-1996) ja toisen sodan (1999-) aikana venäläisten julkisten lähteiden mukaan[59]. Koska kirjoitus perustuu venäläisiin lähteisiin, se välittää nimenomaan hyökkääjän näkemyksen operaation kulusta ja kohdatuista ongelmista.

## Ensimmäinen sota 1994-1996

Ennen sodan alkua Venäjän viestiyhteyspalvelu ja siviilisignaalitiedustelu FAPSI perusti keskuksen Mozdokiin, josta se siirtyi taistelujen alettua Grosznyin lentokentälle. Keskuksella oli kaksi tehtävää: yhdistää asevoimien eri yksiköt siviiliviranomaisiin ja Moskovaan ja toisaalta tukea sotilastiedustelu GRU:n ja sotilaspiirin signaalitiedustelu- ja ELSO-yksiköitä tshetsheenien viestiliikenteen seuraamisessa.

Venäläiset uskoivat tshetsheenien enemmistön ottavan venäläiset vastaan vapauttajina. Venäläisten tiedustelutiedot olivat kaikilta osin erittäin puutteelliset ja operaation kuviteltiin olevan ohi viikossa. Operaation valmisteluihin oli aikaa vain muutamia viikkoja, joten kalusto oli osin epäkunnossa ja joukot olivat edelleen lähes rauhan ajan vahvuudessa.

### *ELSO:n organisointi, toiminta-ajatus ja elektroniselle sodankäynnille käsketyt tehtävät*

Kaikki operatiivis-taktisen tasan signaalitiedustelun ja ELSO:n yksiköt alistettiin federaation voimaryhmittymän elektronisen sodankäynnin päällikölle. ELSO-toiminnan tehtäviksi käskettiin:

- tshetsheenien aseellisten ryhmittyminen viestiverkkojen tiedustelu ja viestiliikenteen suuntautumisen selvittäminen
- tshetsheenien asevoimien johtamisjärjestelmien ja -välineiden, sekä Tshetshenian tasavallan radio- ja TV-kanavien elektroninen lamauttaminen
- elektronisen suojautumisen ja puolustuksen organisointi sekä toteutuksen valvonta
- omien radioelektronisten järjestelmien taajuushallinta[r]

ELSO-joukkojen toiminta-ajatuksena Tshetsheniassa oli lamauttaa havaitut vastustajan kohteet kolmen ELSO-osaston signaalitiedustelulla ja häirinnällä yhdessä samanaikaisten ilmavoimien ja tykistön iskujen kanssa. Tämän ajatuksen mukaisesti käskettiin ELSO-joukoille seuraavat tehtävät:

- lamauttaa HF- ja VHF-yhteydet Groznyista muihin asutuskeskuksiin ja vaientaa Tshetshenian radio- ja TV-kanavat
- saattaa epäjärjestykseen Groznyin puolustus
- katkaista kansainväliset viestiyhteydet Tshetsheniasta

[r] Venäläisessä käsitemaailmassa radioelektronisella taistelulla (REB; radioelektronnaja borba) tarkoitetaan länsimaita laajemmin elektronisen sodankäynnin komponenttien lisäksi myös fyysinen vaikuttaminen samoihin kohteisiin, sekä vahva harhautustoiminta.

Signaalitiedustelun perusteella havaittuja kohteita vastaan iskettiin ilmavoimilla ja tykistöllä. Toiminnan tuloksena tshetsheenijohto oli epäjärjestyksessä kahteen otteeseen useita vuorokausia. Lisäksi katkaistiin kansainväliset yhteydet. Signaalitiedustelulla hankittujen tietojen avulla paljastettiin tshetsheenien aikeet, kokoonpano ja tulevan toiminnan luonne. Tiedoilla onnistuttiin vähentämään merkittävästi federaation joukkojen tappioita. Tshetsheniaa osaavia kielenkääntäjiä ei kuitenkaan ollut riittävästi.

Venäläisten signaalitiedustelu oli jatkuvaa, mutta häirintä ajoitettiin aktiivisten taisteluvaiheiden mukaan. Kaupungeissa yhteyksiin vaikeuttivat tshetsheenien radioasemien lyhyet etäisyydet ja rakennusten katveet. Asutuskeskuksissa vaikeutui myös maalinosoitus signaalitiedustelun suuntimien perusteella. Pääosa tiedustelutiedoista saatiin vastustajan keskusteluja kuuntelemalla. Kaupunkiolosuhteissa tarvittiin toisenlaista kalustoa kuin mitä venäläisillä joukoilla oli käytettävissään. Venäläiset kykenivät kuitenkin sopeutumaan tilanteeseen hankkimalla asutuskeskuksiin soveltuvaa ELSO-kalustoa ulkomailta, mm. Saksasta. Häirinnän lisäksi tshetsheenien johtamistoimintaa häirittiin syöttämällä viestiverkkoihin harhauttavia tietoja.

ELSO-osastojen toimintaa johdettiin federaation joukkojen ELSO-päällikön salatun viestiverkon kautta. Ennen seuraavan hyökkäysvaiheen alkua radioverkkojen kutsut saatiin yhdistettyä eri johtoportaisiin ja johtajiin. Signaalitiedustelun onnistui näin selvittää tshetsheenien tiedustelun ja valvonnan johtamisjärjestelmä, operatiivinen johtamisjärjestelmä ja taktiset johtoverkot.

Federaation omien viestiyhteyksien toiminnan varmistamiseksi järjestettiin taajuushallinta asevoimien ja muiden ministeriöiden eri yksiköiden välillä. Myöhemmin taajuushallinnan ylläpito oli jatkuvaa uusien yksiköiden tullessa alueelle. Erillinen tarkkailuyksikkö valvoi jatkuvasti taajuushallinnan ja viestiliikenneohjeiden noudattamista.

### *Käytettävissä ollut ELSO-voima*

Tshetshenian lähistölle (Mozdokiin ja Vladikavkaziin) siirrettiin elokuussa 1994 1919. erillinen ELSO-pataljoona, 1077. erillinen signaalitiedustelupataljoona, 42. AK:n ELSO-joukot ja 286. erillinen häirintähelikopterilentue.

Sotilaspiirin signaalitiedusteluyksikön neljä viestitiedusteluasemaa tukivat operaatiota. Budjonnovskin ja Mozdokin kentillä oli 30 minuutin lähtövalmiudessa häirintähelikopterilentue. ELSO-toimintaa johdettiin Mozdokin kentällä sijainneelta komentopaikalta.

### *Taistelujaotus ja tehtävät ELSO-yksiköille*

Myöhemmin 8. AK:n organisaatioon kuulunut ELSO-ryhmä keskitettiin tukikohtaan kaksi kilometriä Tolstoi-Jurtista itään. Signaalitiedustelu- ja VHF-häirintäyksiköt ryhmitettiin Terek-harjanteelle. ELSO-toimintaan liittyi taistelun kaikissa vaiheessa tulen käyttö. 42. AK:n ELSO-joukot vastasivat signaalitiedustelusta ja häirinnästä

Groznyin länsipuolella. Taisteluajatuksen mukaisesti Läntiseen ja Pohjoiseen ryhmään perustettiin signaalitiedustelu- ja ELSO-ryhmät. Mozdokiin jäi reserviin 42. AK:n ELSO-osasto. Yksiköille annettiin 25 häirintäasemaa ja 42 signaalitiedusteluasemaa. Venäläisten ELSO:n kohteena oli myös Tshetshenian asutuskeskusten ja naapuritasavalloissa toimivien agenttien välinen radioliikenne, jossa välitettiin tiedustelutietoja federaation joukkojen liikkeistä ja toiminnan luonteesta.


**Kuva 50: Tshetshenian alue ja venäläisten kolme pääetenemissuuntaa.**

Venäläiset alistivat taistelujaotuksessaan ELSO-komppanioita yhtymille, jotta elektronisella sodankäynnillä kyettäisiin tukemaan iskeviä osia mahdollisimman pienin viipein. Toisin kuin erillisten ELSO-pataljoonien, niiden tehtävänä ei ollut hankkia tiedustelutietoa, vaan tukea iskevää osaa tilannekuvan muodostamisella ja maalinosoituksella. Varsinaisten sotatoimien päätyttyä kaikki ELSO-yksiköt keskittyivät signaalitiedusteluun ja häirintään.

### *ELSO-tuli-iskun toteuttaminen*

Käsketystä hetkestä alkaen tshetsheenien viestiyhteydet sekä radio- ja TV-kanavat lamautettiin aluksi 2-4 tunniksi vuorokaudessa ja myöhemmin 6-8 tunniksi. Tässä vaiheessa ilmavoimat pommitti Tshetshenian lentokenttiä ja tuhosi kaiken

konekaluston, poltto- ja voiteluainevarastot, lennonjohtopaikat ja lennonvarmistusjärjestelmän antennit. Samanaikaisesti kuvattiin lentotiedustelulla joukkojen tulevat hyökkäysurat. Tiedustelulennoilla noudatettiin radiohiljaisuutta ja kuvaustulokset toimitettiin analysoitavaksi lentokuljetuksin.

Tärkeimmät tshetsheenien VHF-alueella toimivat verkot voitiin havaita vain IL-20M -lentokonejärjestelmällä. Puheradioverkoissa käytettiin venäjää tai tshetsheniaa, ja tiedustelua vaikeutti tshetsheniaa osaavan henkilöstön puute. Analysoitujen signaalitiedustelun havaintojen perusteella sotilaspiirin ELSO-upseerit pitivät kerran vuorokaudessa tilannekatsauksen yläjohtoportaalle.

Tshetsheenien operatiivisen johdon ja opposition radioverkkoja seurattiin eri viestitiedustelujärjestelmillä. Tshetsheenit käyttivät rajoitetusti HF-radioita operatiivis-taktisten tietojen välittämiseen ennen varsinaisen sodan alkua. Vasta marraskuussa 1994 HF-liikenne lisääntyi ja tshetsheenit alkoivat käyttää mm. radioamatöörilaitteita. Näissä verkoissa toimi myös muissa Kaukasian tasavalloissa sijaitsevia asemia.

Tshetsheenit käyttivät paljon myös muiden ministeriöiden viestivälineitä, radiolinkkejä ja jopa matkapuhelimia. Pääosa kalustosta oli neuvostovalmisteista, minkä lisäksi tshetsheenit ostivat ulkomailta runsaasti uusia kannettavia viestilaitteita. Tshetsheenit sijoittivat Groznyin kaupunkiin toistinasemia, ja itse kaupunkiin perustettiin radioharhautusyksikkö.

**Kuva 51: Venäläinen Il-20M-signaalitiedustelukone. Koneen antenneja on sijoitettu koneen alla ja sivulla näkyviin säiliöihin ja antennisuojiin.** [© Jane's 2004]

***Maahyökkäyksen tukeminen***

Venäjän joukot siirtyivät Tshetshenian alueelle kolmesta suunnasta, ja ELSO-yksiköt ryhmitettiin etupainoisesti heti pääjoukkojen ensimmäisen portaan pataljoonien jälkeen. Tehtävään määrätyt häirintäasemat toimivat sekä liikkeestä että aina marssijoukon pysähtyessä. Mozdokiin jäänyt ELSO-reservi vastasi signaalitiedustelusta ja lamauttamisesta läntisessä suunnassa.

***Puolustajan toiminta ja ELSO:n vaikutus siihen***

Venäläiset onnistuivat etenemisensä aikana häiritsemään sekä tshetsheenien HF- että VHF-yhteydet, minkä seurauksena nämä väistivät toisille taajuuksille. Tshetsheenit oppivat kuitenkin toimimaan venäläisten käyttämillä taajuuksilla siten, että he käyttivät hyväkseen venäläisten radioliikenteen taukoja. Tshetsheenien radioliikenne koostui pääosin federaation joukkoihin liittyvistä tiedustelutiedoista.

**Kuva 52: Venäläinen Mi-8 ”Hip K” -häirintähelikopteri. Kopterin takasivulla näkyvät viestijärjestelmien häirintään tarkoitetut ristin muotoon ryhmitetyt dipoliantennit.** [© Jane’s 2004]

Tshetsheniassa taktiset johtoportaat (joukkue-rykmentti) joutuivat toimimaan yleensä itsenäisesti, mutta venäläisten organisaatio, kalusto ja taktiikka eivät kyenneet vastaamaan uusiin haasteisiin. Luotettava viestiyhteys ilmavoimiin, ylempään johtoportaaseen ja naapuriyksiköihin oli tässä tilanteessa elintärkeää. Taistelujen alkaessa nykyaikaisten radioiden sekä salainten ja puheensekoittajien tarve kasvoi jyrkästi. Venäläiset pyrkivät suojaamaan viestiliikennettään tshetsheenien kuuntelutiedustelulta, häirinnältä ja harhauttamiselta käyttämällä salausta. Ongelmana oli kuitenkin salauslaitteiden ja myös päätelaitteina käytettävien kannettavien tietokoneiden puute.

Salainten käytössä ja viestiliikenneasiakirjojen (peitteistöt, avaimistot) jakelussa oli myös ongelmia. Suurelta osin federaation joukkojen viestijärjestelmät olivat vanhanaikaisia ja ilman salausta.

Kokemukset Groznyin taisteluista osoittivat, että taktisissa johtoverkoissa on ehdottomasti käytettävä salausta – tshetsheenit kykenivät seuraamaan vaivatta venäläisten radioliikennettä. Radio-, linkki- ja salaamattomien puhelinyhteyksien kanssa on ehdottomasti käytettävä puheenpeittämis- ja johtamistaulukoita, joiden koodit on muutettava vähintään kerran vuorokaudessa. Oma johtamisjärjestelmä on suojattava muuttamalla useasti viestiliikenneperusteita tietovuotojen estämiseksi.

Tykistön tulenjohtoyhteydet vetivät tshetsheenien tulen puoleensa, joten tulenjohtoon käytettiin yleensä kenttälinkki- ja kaapeliyhteyksiä. Lentotulenjohtajilla ei ollut tähän mahdollisuutta ja he olivat tshetsheenien pääkohteina. Lentotulenjohtajat oli helppo tunnistaa ja paikantaa käsisuuntimoilla, koska radioissa ei käytetty salaimia.

Strategisia ja operatiivis-taktisia signaalitiedusteluyksiköitä käytettiin niille sopimattomiin tehtäviin, koska signaalitiedustelun järjestelmät oli alistettu ELSO-päällikölle, eikä tiedustelupäällikkö saanut niiltä käytännössä lainkaan tiedustelutietoja. Tämä johti siihen, että ELSO-päällikkö välitti taisteleville joukoille ristiriitaisia ja jopa vääriä tietoja, joita ei oltu vahvistettu muista lähteistä. Tiedustelun toimintaa vaikeutti lisäksi heikko yhteistyö asevoimien sisällä ja muiden voimavirastojen välillä.

Kaikkia operaatiota tukemaan tarvittiin ELSO-yksiköitä. Operaation varatut resurssit eivät kuitenkaan olleet riittäviä annettuihin tehtäviin nähden useasta eri syystä:

- Signaalitiedustelun yksiköt joutuivat sotaan lähes rauhan ajan kokoonpanossa (25-30% sodan ajan vahvuudesta).
- Henkilöstön koulutustaso oli heikko.
- Nykyaikaisesta signaalitiedustelukalustosta oli puutetta.
- IL-20-signaalitiedustelukoneen järjestelmä oli pahasti vanhentunut eikä sillä ollut salattua yhteyttä maa-asemaan, mikä viivästytti havaintojen käsittelyä jopa 4 tuntia.

## Toinen sota 1999 alkaen

Toisessa Tshetshenian sodassa ensimmäisen sodan kokemuksista otettiin oppia, ja uuden kaluston sekä taktiikan lisäksi tiedotusvälineiden toimintavapautta rajoitettiin jyrkästi. FAPSI ja GRU olivat seuranneet tshetsheenejä jatkuvasti sotien välisen ajan. FAPSI oli lisäksi jättänyt vuonna 1997 poistuessaan Groznyin kentältä satelliittikeskuksensa toimintakuntoisena tshetsheenien käyttöön. FAPSI pystyi kuitenkin seuraamaan sen läpi kulkenutta viestiliikennettä.

Toisen Tshetshenian sodan alussa tshetseenien viestijärjestelmät olivat pääosin hyvin vanhanaikaisia, ja niistäkään useita ei käytetty lainkaan toiminnan salaamiseksi.

Tshetsheenien tutkista, matkapuhelintukiasemista ja linkeistä suurin osa oli tuhottu jo ensimmäisessä sodassa. Tukiasemia oli korvattu länsimaisilla radiopuhelimilla, ulkomailta ostetuilla linkeillä ja yleisradiolähettimillä. Näistä pääosa tuhottiin heti toisen sodan alussa. Tshetsheenit ovat käyttäneet runsaasti kaupallisia satelliittipuhelimia toisen sodan aikana, mikä mahdollisti yhteydet myös Internet-verkkoon.

Dagestanin ja Ingushetian lähistöllä tshetsheenit käyttivät hyväksi näiden tasavaltojen NMT-450-tukiasemia, joiden avulla oli luotu 20-60 ala-asemaa käsittävä tiedustelu- ja valvontaverkko. Lisäksi sissiryhmillä oli radiopuhelimia ja GPS-paikantimia. HF-alueella toimi 60-80 aseman tiedustelu- ja valvontaverkko, joka käytti kenttäradioita, radioamatöörilaitteita ja kansainvälisiltä avustusjärjestöiltä vietyjä laitteita. Tshetsheeneillä oli lisäksi käytössään akustisia ja signaalitiedustelujärjestelmiä. Tshetsheenikomentajilla oli TV-lähettimiä, joiden kantama oli 20-30 km ja joita käytettiin harhauttamiseen ja psykologiseen sodankäyntiin.

Venäläiset aliarvioivat sekä tshetsheenien tiedustelu- ja valvonta- että johtamisjärjestelmien tehon. Vielä toisen sodan alussa tshetsheenit kykenivät paikantamaan suuntimoverkkonsa avulla venäläisten johtamispaikat ja tuliasemat.

Venäläisten signaalitiedustelulla ei toisen sodan alkuun mennessä ollut seurattavia kohteita, lukuun ottamatta tshetsheenien Inmarsat-puhelimia ja kenttäkomentajien radioverkkoja. Venäläiset uskoivat tuhonneensa kaikki tshetsheenien tutkat, joten elektronista mittaustiedustelua ei tehty ja vasta syyskuussa 1999 federaation ilmavoimat havaitsi Tshetsheniassa tutka-aseman, jonka tuhosi nopeasti.

Lokakuussa 2003 siirryttiin Tshetsheniassa signaalitiedustelun ja ELSO-toiminnan osalta uuteen vaiheeseen, kun venäläiset ilmoittivat, että ”elektronisen sodankäynnin joukoilla ei ole enää maaleja”. Tshetsheenijohto oli tullut erittäin varovaiseksi, ja venäläisjoukkojen parantuneen signaalitiedustelukyvyn vuoksi he olivat käytännössä lopettaneet radioiden, matkapuhelimien ja satelliittipuhelimien käytön johtamisessa. Tshetsheenien välttäessä radioiden käyttöä tiedustelussa käytettiin aiempaa enemmän tavanomaisia menetelmiä ja uusia Ptshela-1T-lennokeita. Vuoristossa tiedustelun apuna olivat tiedustelulentokoneet ja GRU:n tiedustelusatelliitit.

## Venäläisten kehittämiskohteet ensimmäisen sodan jälkeen ja niiden huomiointi toisen sodan aikana

Venäläiset näkivät ensimmäisestä Tshetshenian sodasta saatujen kokemusten perusteella seuraavien osa-alueiden vaativan kehittämistä[60]:

1. Parempi yhteistyö asevoimien sisällä ja toisaalta eri voimavirastojen kanssa. Yhteistyötä on tehostettu mm. sijoittamalla yhteysupseereita ja vaihtamalla viestivälineitä.

2. Signaalitiedusteluyksiköiden henkilöstön on oltava käytössä jo rauhan aikana, hyvissä ajoin ennen varsinaisen kriisin alkua. Maavoimien upseeristo ei ole

osannut käyttää tiedustelua puutteellisen koulutuksen vuoksi. Toisessa sodassa tiedustelu on ollut ensimmäistä sotaa tehokkaampaa, mutta ei läheskään riittävää. Tiedusteluhenkilöstön on jo operaation käynnistysvaiheessa kyettävä toimimaan 24 tuntia vuorokaudessa; taistelutilanteessa jopa kolmasosa toiminnasta on tapahtunut yöaikaan.


**Kuva 53: Venäläiset käyttivät jo syyskuussa 1999 signaalitiedustelu-, TV- ja infrapunasensorein varustettua Stroy-P-lennokkijärjestelmää, jonka lennokkina käytettiin Ptshela-1T:tä.** [© Jane's 2004]

3. Vastustajan syvyydessä olevien kohteiden tiedusteluun on oltava jo rauhan aikana lentävä tai satelliittitiedustelujärjestelmä. Signaalitiedustelukoneet ovat toimineet alueella jatkuvasti. Signaalitiedustelu-, TV- ja infrapunasensorein varustettu Stroy-P-lennokkijärjestelmä (lennokkina em. Ptshela-1T) toimitettiin Tshetshenian lähialueelle jo syyskuussa 1999.

4. Omien joukkojen on noudatettava viestiliikennekuria ja käytettävä salaimia jo rauhan aikana viestivälineestä riippumatta (kaapeli-, radio-, satelliitti-, troposironta- ja kenttälinkkiyhteyksillä). Sodan alusta alkaen venäläiset ovat rikkoneet jatkuvasti viestiliikennemääräyksiä, ja ainoaksi varmaksi keinoksi suojata yhteydet on todettu automaattinen salauksen käyttö. Uusien radioiden lisäksi vanhoja kenttäradioita on varustettu puheensekoittajilla.

5. Taistelujen alusta lähtien vastustajan tiedustelu-, valvonta- ja johtamisverkot on lamautettava mahdollisimman pysyvästi. Vielä toisen sodan alussa tshetsheenien signaalitiedustelun suorituskyky aliarvioitiin, joten venäläisten

ELSO ei kyennyt lamauttamaan tshetsheenien tiedustelu- ja valvontaverkkoja. Tiedot venäläisten joukkojen siirroista, johtamispaikoista, tuliasemista ja huollon kohteista päätyivät tshetsheeneille, jotka saattoivat näiden perusteella suunnitella toimintaansa. Vasta tammikuussa 2003 federaation joukot ilmoittivat, että tshetsheenien toiminta radioverkoissa on vähentynyt jyrkästi, eivätkä aseellisten ryhmien johtajat ole äänessä juuri lainkaan

6. Signaalitiedustelun on kyettävä paikantamaan vastustajan johtamispaikat tarkkuudella, joka riittää epäsuoran tulen ja ilmatulen tulenjohtoon eli kohteet on voitava tuhota signaalitiedustelun antaman maalinosoituksen perusteella. Tshetsheniassa on otettu operatiiviseen käyttöön uusi tiedustelujärjestelmä Vega ja ELSO-järjestelmä Arbalet-MG, joiden antaman maalinosoituksen avulla on lamautettu sissien johtamisyhteydet neljällä vuoristoalueella iskemällä kohteisiin tykistön ja ilmavoimien tulella. Federaation joukoille on vuonna 2004 toimitettu tuhansia GLONASS-järjestelmää käyttäviä paikantimia, mikä on lisännyt huomattavasti epäsuoran tulen nopeutta, tarkkuutta ja tehoa.

7. Signaalitiedustelu-, ELSO- ja viestiyksiköiden koulutus on järjestettävä tehokkaasti jo rauhan aikana, koska niiden täydennyskoulutukseen ei ole enää aikaa tilanteen kiristyessä. Viestijoukkojen koulutustaso on selvästi parantunut koko Venäjän alueen käsittävien esikunta- ja johtamisharjoitusten sekä kaksi kertaa vuodessa järjestettävien viestisotaharjoitusten avulla.

8. Vastustajan kieltä osaavan henkilöstön rekrytointi. Venäläisten puolella taistelee toisessa sodassa suuri määrä tshetsheenejä, mutta luotettavuus-ongelmat vaikeuttavat heidän käyttöään erikoistiedustelun tehtävissä.

9. Kaupunkitaisteluihin ja paikallisiin konflikteihin sopivien, salaimilla varustettujen kevyiden kenttäradioiden ja matkapuhelimien kehittäminen. Kaupunkioloissa vastustajan on helppo lamauttaa johtamisyhteydet: kenttälinkkiyhteydet eivät ole toimineet, mutta johdinyhteydet toimivat. Venäläisjoukoille tuli uusi tuhatmäärin jaettu, salaimella varustettu Akveduk-radioperhe, jota tshetsheenit eivät enää kyenneet kuuntelemaan. Lisäksi FAPSI on rakennuttanut suojatun viranomaisverkon mm. Tshetsheniaan. Sen ensimmäiset salaimilla varustetut puhelimet toimitettiin alueelle lokakuussa 2002.

10. Satelliitti- ja kenttälinkkijärjestelmät on sijoitettava panssaroituihin ajo-neuvoihin, eikä kalliita viesti-, tiedustelu- ja johtamisjärjestelmiä ole järkevää sijoittaa halvalle alustalle. Johtamis- ja viestijärjestelmien alustoina on käytetty BTR-80- ja BMP-1KShT-ajoneuvoja komppania-joukkue tasalle asti. Joukoille on jaettu uusia maastonvalvontatutkajärjestelmiä Fara-1, Monitor-M ja Credo 1E.

11. Signaalitiedusteluyksiköillä ja ELSO-yksiköillä on oltava omat tehtävät ja johtoportaat, mutta niillä on oltava mahdollisuus reaaliaikaiseen maalitiedon

vaihtoon. Signaalitiedustelun yksiköt on alistettu muiden tiedusteluyksiköiden tavoin tiedustelupäällikölle ja ELSO-yksiköt ELSO-päällikölle. Tiedonsiirtoon pataljoonien ja rykmentin komentopaikkojen välillä on olemassa järjestelmä, ja uusilla kenttäradioilla on maalin koordinaatit voitu välittää suoraan ampuville yksiköille.

**Kuva 54: Venäläisten Vega (85V6-A) -tiedustelujärjestelmän Orion-mittaus-tiedusteluasema. Järjestelmän eri taajuusalueen antennit on sijoitettu mastoon, suuntiminen tehdään antennirakennelmaa pyörittämällä.**

12. Operaatiotaitoa ja taktiikkaa on kehitettävä – paikallisessa sodassa toimivat erilaiset lainalaisuudet kuin laajamittaisessa sodassa. Toisessa sodassa on kehitetty tiedustelu- ja iskuosastotoimintaa, jossa tiedustelun maalinosoituksen perusteella kohde tuhotaan kaukovaikutteisin asein. Tällöin omat tappiot jäävät hyvin pieniksi.

13. ELSO:n ja maalitiedustelun on oltava osa kaikkea tulenkäytön suunnittelua. Tappioiden välttämiseksi maavoimat ei iske vastustajan kohteisiin ilman tykistön tai ilmavoimien ja taisteluhelikoptereiden tukea. ELSO-yksiköitä käytetään vastustajan paikantamiseen ja johtamisyhteyksien lamauttamiseen. Tuhottavia kohteita valvotaan jatkuvasti lennokeilla, helikoptereilla, viesti-tiedustelua ja muilla teknisillä välineillä.

Toisesta Tshetsheniaan tehdystä hyökkäyksestä saatujen kokemusten perusteella elektronista sodankäyntiä pidettiin edelleen tärkeimpänä kehitettävänä alueena. Tämä näkyy myös asevoimien budjetissa: esimerkiksi vuonna 2003 materiaalihankkeisiin käytettävästä lähes 70 miljardista ruplasta noin 42% käytetään elektroniseen sodankäyntiin[61].

## Johtopäätöksiä historiasta

Yleisenä havaintona asevoimien suhtautumisesta elektroniseen sodankäyntiin voidaan todeta, että syvän rauhan tilan aikana armeijat byrokratisoituvat ja ”virkamiesmäistyvät” keskittyen rauhan aikaiseen toimintaan ja unohtaen samalla sodan ja taistelun realiteetit. Tämä ilmiö tuntuu vaivaavan kaikkien maiden asevoimia, mutta erityisen korostunut se on asevoimille, jotka kokevat voittaneensa edellisen sodan eivätkä sen vuoksi tunne tarvetta kehittää sodan ajan suorituskykyään radikaalisti paremmaksi.

Järjestelmiä hankitaan yhä enemmän niiden näennäiseen suorituskykyyn tuijottaen ja varsin rauhanomaisissa sotaharjoituksissa saatuihin kokemuksiin luottaen. Suoritus-kykyvaatimuksissa, teknisissä spesifikaatioissa, järjestelmätesteissä ja henkilöstön koulutuksessa laiminlyödään tai jopa unohdetaan vastustajan vaikutus. Sitten kriisin puhjettua ja viimeistään taisteluiden alettua on jouduttu kohtaamaan ikäviä yllätyksiä, kun ase, sensori tai tiedonsiirtojärjestelmä ei toimikaan vastustajan häirinnän vuoksi, tai ne tuhotaan paljon ennen kuin ne ovat kyenneet hyödyntämään näennäistä suorituskykyään. Mikäli aikaa on ja tilanne sen sallii, ryhdytään kiireen vilkkaa tuottamaan häirintä- ja omasuojajärjestelmiä sekä asentamaan niitä järjestelmiin. Joissakin tapauksissa on päädytty jopa modifioimaan aselavetteja, kuten pommi- ja rynnäkkökoneita, elektronisen sodankäynnin alustoiksi. Parempi vaihtoehto olisi pyrkiä tuottamaan jo lähtökohtaisesti sodan ajan suorituskykyä ja välttää keskittymästä rauhanaikaiseen näennäiseen tekniseen suorituskykyyn.

# 8. YHDISTELMÄ JA JOHTOPÄÄTÖKSET

Elektroninen sodankäynti on rauhan aikana suunnittelua, varustamista, koulutusta ja harjoittelua. Järjestelmien toimivuus koetellaan vasta kriisitilanteessa – siihen asti elektroninen sodankäynti on rahanmenoa, lisätyötä ja jatkuvaa ongelmien ratkomista.

***Tekniikan merkitys ylivoiman lähteenä on ELSO:n myötä noussut merkittäväksi.***

Yhteiskunnan ja sodankäynnin teknistymisen myötä teknologian merkitys sodankäynnissä on ratkaiseva. Elektroninen sodankäynti on pohjimmiltaan tekniikan kaksintaistelua sähkömagneettisen spektrin kautta. Taktiikka, operaatiotaito ja strategia kuitenkin määrittävät, miten tekniikkaa hyödynnetään sodankäynnissä. Näiden yhdistelmä tarjoaa mahdollisuuden luoda vallankumouksellista suorituskykyä. Sotilaalliset vallankumoukset muodostuvat aina kolmesta tekijästä: uuden tekniikan käyttöönotosta ja uudesta tavasta organisoida ja käyttää sotilaallista voimaa[62,s]. Radikaali muutos edellyttää siten tekniikan, organisaation ja doktriinin yhtäaikaista ja yhdenmukaista kehittämistä ja käyttöönottoa[63]. On kuitenkin huomattava, että nimenomaan tekniikka luo edellytykset taktiikalle, operaatiotaidolle ja strategialle. Tekninen etumatka vastustajaan voi kompensoida taktisia heikkouksia, ja vastaavasti vastustajaa parempi taktiikka voi kompensoida teknistä alivoimaa, mutta vain tiettyyn rajaan asti. Parhaallakaan taktiikalla tai taisteluhengellä ei voida korvata suuria puutteita tekniikassa.


Taistelun johtajan on tunnettava elektronisen sodankäynnin vaikutus sotilaallisiin operaatioihin, vastustajan elektronisen sodankäynnin järjestelmien suorituskyky ja käyttöönsä annettujen elektronisen sodankäynnin joukkojen oikeat käyttöperiaatteet.

[s] Esimerkiksi saksalainen salamasota muodostui tekniikan, doktriinin ja organisaation uudistuksista, joista mikään ei olisi yksinään muodostanut radikaalia muutosta. Tekniikkaa edusti johtamisjärjestelmän (radioiden laajamittainen käyttöönotto), syvän täsmäasevaikutuksen (Ju-87-syöksypommittaja) ja operatiivisen liikkuvuuden (panssarijoukot sekä kuorma-autoilla liikkuva jalkaväki ja motorisoitu tykistö) kehittäminen. Doktriinia puolestaan edusti siirtyminen liikkuvaan sodankäyntiin ja iskeminen vastustajan voiman lähteille. Panssaridivisioona luotiin itsenäiseksi organisaatioksi, joka hyökkäyksen keihäänkärkenä kykeni nopeisiin iskuihin vastustajan syvyyteen.

Komentajat ja esikuntaupseerit on koulutettava hyödyntämään ELSO:a kokonaisvaltaisesti ja ottamaan vastustajan ELSO sekä uhkana että maaleina huomioon operatiivisissa suunnitelmissa. Länsimaissa on havaittu, että ***ELSO:n tehokkaan käytön suurimpana esteenä on korkeimpien upseereiden heikko ELSO-tuntemus.*** Sen vuoksi elektroninen sodankäynti tulee sisällyttää kaikkeen taistelun johtamista käsittelevään koulutukseen.

***Elektronisen sodankäynnin suunnittelun ja johtamisen on oltava kiinteä osa operaation suunnittelua jo toteuttamista***. Pahimmat virheet ovat ELSO:n pitäminen erillisenä ”nörttien” miehittämänä alueena operaatiosuunnitelmissa ja operaatioiden toteuttamisessa, sekä ELSO:n rajaaminen koskemaan vain informaatio-operaatioita tai informaatiosodankäyntiä, johon se puolustusvoimien määritelmien mukaan kuuluu. ELSO on pidettävä riittävän itsenäisenä. ***ELSO:a ei saa sulauttaa informaatio-sodankäyntiin***, vaikka se sitä tukeekin

Sodankäynnin teknistyessä elektronisen sodankäynnin merkitys tulee ratkaisevaksi: ilman sitä taistelu on tuomittu häviöön. Teknisesti alivoimaisen on äärimmäisen vaikeata voittaa, vaikka operaatiotaito ja taistelutekniikka olisivatkin kohdallaan. Jos ohjus ei osu, tutka ei näe eikä radiosta kuulu kuin kohinaa, taistelua on lähes mahdotonta voittaa millä tahansa taktiikalla. Toisaalta, jos vastapuoli ei saa ohjuksiaan osumaan, tai kykene johtamaan taisteluaan, on merkittävästi alivoimaisenkin osapuolen mahdollista voittaa, mikäli kykenee hyödyntämään tätä suhteellista etuaan omassa operaatiotaidossaan.

***Sodankäynnissä mikään ei ole pysyvää. Tekninen tai taktinen etu voi olla olemassa päivän, viikon, tai jopa muutaman vuoden, mutta ei ikuisesti. Tämän oppii yleensä vain hävinnyt osapuoli, jonka on pakko oppia.***

Kaikki merkittävä joutuu sodankäynnissä hyökkäyksen ja puolustuksen kohteeksi. Mitä enemmän sodankäynnissä käytetään sähkömagneettista spektriä, sitä enemmän myös vastatoimet kehittyvät. Digitaalielektroniikka ja informaatioteknologia mahdollistavat uusien järjestelmien tai ominaisuuksien nopean kehittämisen ja käyttöönoton. Toisaalta myös vastatoimenpiteiden kehittäminen on yhtä nopeata. Elektronisten vastatoimien nopeasta syntymisestä seuraa, että sotilaallinen etu ei ole pysyvä. Tekninen tai taktinen etu voi olla olemassa päivän, viikon, tai jopa muutaman vuoden, mutta ei ikuisesti. Tämän oppii yleensä vain hävinnyt osapuoli, jonka on pakko oppia. Esimerkiksi kelpaa vuoden 1967 sota, jossa egyptiläiset tuhosivat neljällä ammutulla ja maaliinsa osuneella Styx-merimaaliohjuksella israelilaisen Eilat-hävittäjän. Kuusi vuotta myöhemmin Israelin panostettua elektroniseen suojautumiseen syyrialaiset ampuivat kuutisenkymmentä ohjusta osumatta yhteenkään israelilaiseen alukseen. Vastaavasti israelilaisten Gabriel-ohjukset upottivat 17 arabien alusta. Syyrialaisten massiiviset investoinnit uusiin aseisiin valuivat täysin hukkaan niiden ELSO-keston laiminlyönnin vuoksi. ***Suhteellisen edun ylläpito muuttuvassa ympäristössä edellyttää sekä pitkäjänteistä osaamisen kehittämistä ja ylläpitoa, että kykyä kehittyä nopeammin ja joustavammin kuin vastustaja.***

Puolustusvoimat on ryhtynyt 2000-luvulla panostamaan elektroniseen sodankäyntiin. ELSO ja siihen läheisesti liittyvät häivetekniikka, informaatiosodankäynti ja johtamisjärjestelmätekniikat on määritetty puolustusvoimien kannalta kriittisiksi osaamisalueiksi eli alueiksi, joiden hallinta on maamme puolustuksen kannalta keskeistä ja joilla kansallisella panostuksella voidaan saavuttaa merkittävää strategista ja operatiivista etua. ***ELSO on kustannustehokkain tapa lisätä järjestelmäkokonaisuuden suorituskykyä tai saavuttaa sama suorituskyky huomattavasti pienemmillä kappalemäärillä.***

***Elektroninen sodankäynti on alue, jonka osaaminen yhtyy Suomen ydinosaamisalueisiin ja jossa pieni, mutta teknologisesti kehittynyt valtio, jonka asevoimat soveltavat innovatiivista taktiikkaa ja kykenevät nopeasti sopeutumaan toimintaympäristöönsä, voi saavuttaa laadullisen ylivoiman vastustajasta.*** Toisaalta uhkaympäristössä ja potentiaalisilla operaatioalueilla oleva ELSO-suorituskyky muodostaa erittäin keskeisen uhkan omalle jatkuvasti teknistyvälle kokonaisjärjestelmällemme, jonka elektronisen suojaamisen lisäksi on varmistettava riittävien varajärjestelmien toiminta.

Elektronisen sodankäynnin järjestelmien teknistä kehitystä ohjaa matkapuhelinteknologian vetämä radiotekniikan yleinen tekninen edistys ja massatuotannon mukanaan tuoma yksikkökustannusten laskeminen. Elektronisen sodankäynnin järjestelmissä elektronisen tuen ja elektronisen vaikuttamisen ominaisuudet integroituvat samoihin järjestelmiin: taktinen tiedustelu- ja valvontajärjestelmä kykenee tulevaisuudessa useissa tapauksissa myös häiritsemään havaitsemiaan kohteita. Riittävän suuritehoisen häirintäsignaalin kohdistaminen maaliin edellyttää häirintäjärjestelmältä kykyä seurata häirittävää maalia. Integroituminen voi tapahtua joko fyysisesti tai toiminnallisesti taistelukentän verkottumisen kautta.

***Kyky suojautua täsmäaseilta jakaa armeijat toimintakykyisiin ja toimintakyvyttömiin.***

Täsmäaseiden vaikutus sodankäyntiin on keskeinen: ne mahdollistavat yhteiskunnan ja asevoimien infrastruktuurin lamauttamisen nopeasti ja suhteellisen pienin voimin. Halvat täsmäaseet muuttavat myös linnoittamisen ja esimerkiksi siltojen, huoltokeskusten yms. suojaamisen merkitystä ja toteutusta perinteisestä linnoittamisesta. Kyky käyttää täsmäaseita jakaa tulevaisuudessa armeijat tehokkaisiin ja tehottomiin siinä missä kyky suojautua täsmäaseilta jakaa ne sodassa toimintakykyisiin ja toimintakyvyttömiin. Asejärjestelmältä suojautumista ei voi jättää yksin elektronisen ja fyysisen suojautumisen varaan: suojautumisen lisäksi on kyettävä vaikuttamaan vastustajaan niin fyysisesti kuin elektronisestikin. Näiden yhdistelmällä voidaan suojautua vastustajan tiedustelu- ja valvontajärjestelmältä sekä asevaikutukselta.

***Pelkkä elektroninen suojautuminen ei riitä: on kyettävä myös vaikuttamaan.***

***Tulevaisuuden keskeisin kysymysmerkki on suunnatun energian aseiden merkitys sodankäynnille***. Radiotaajuiset aseet tarjoavat mahdollisuuden vastustajan tutka- ja radiolinkkijärjestelmien tuhoamiseen sekä erittäin tehokkaiden omasuojajärjestelmien

kehittämiseen. Suunnattu infrapunahäirintä ja -sokaisu puolestaan mahdollistaa infrapunahakuisten ohjusten sekä lämpötähtäinten ja optronisten maalinosoitus-järjestelmien lamauttamisen. ***Tekninen kehitys saattaa siten tehdä suuresta osasta taistelukentän järjestelmistä käyttökelvottomia, ellei vastatoimien kehittämiseen uhkan tahdissa kiinnitetä riittävästi huomiota***[64].

2000-luvun alussa alkoi esiintyä tietoja entisen Neuvostoliiton alueelta tulleiden palkkasotureiden käytöstä elektronisen sodankäynnin alueella, erityisesti elektronisen tuen sensoreiden operaattoreina ja operatiivisen suunnittelun sotilasasiantuntijoina. Siten kriisinhallinta- ja rauhanturvaoperaatioissakin vastustajalla voi olla käytössään moderneja elektronisen sodankäynnin välineitä. On myös nähtävissä, että ELSO leviää siviiliyhteiskuntaankin: poliisi- ja rajavartioviranomaisten käyttöön tulee elektronisen tuen järjestelmiä, poliisille ollaan länsimaissa kehittämässä elektroniikkaa lamauttavia välineitä, kriisialueilla lentäviin matkustajakoneisiin ollaan asentamassa omasuoja-järjestelmiä terroristien käyttämiä olkapääohjuksia vastaan, tietokone- yms. laitetiloja ollaan suojaamassa radiotaajuisilta aseilta ja kriisinhallintaoperaatiossa toimivia sotilaita ja siviilejä suojataan radiolla laukaistavilta tienvarsi- ja autopommeilta[65,66]. Elektroniikan kahtaiskäyttö (siis saman teknologian käyttö sotilas- ja siviili-tarkoituksiin) tai puhdas siviilikäyttö laskee teknisten toteutusten hintoja, mutta teknisesti vaativimmat sovellukset säilyvät kuitenkin asevoimien käytössä.

Viime vuosina maailmalla on panostettu huomattavasti informaatiosodankäynnin ja informaatio-operaatioiden kehittämiseen. Elektroninen sodankäynti on tällöin nähty lähinnä informaatiosodankäynnin osa-alueena. Vaikka elektronisen sodankäynnin suunnittelun ja johtamisen onkin oltava osa informaatio-operaation suunnittelua ja toteuttamista, elektronista sodankäyntiä ei kuitenkaan saa pelkistää informaatio-sodankäynnin alalajiksi, vaan se tulee nähdä itsenäisenä elementtinä, joka tukee informaatio-operaatiota.

Suomalaisessa sodankäyntikonseptissa näkyy varautuminen toimimaan tuli- ja spektri-alivoimatilanteessa. Tällöin on kyettävä toimimaan suojassa ja vaikuttamaan vastustajan kriittisiin osiin. Elektroninen sodankäynti luo mahdollisuuden ylivoimaiseen tekniseen suorituskykyyn ja avaa uusia operatiivisia mahdollisuuksia lukumääräisesti ylivoimaisen vastustajan lyömiseen. Suomalaisessa sodankäynnissä on käytettävä epäkonventionaalista operaatiotaitoa ja tekniseen ylivoimaan perustuvia epäsymmetrisiä ratkaisuja. On kyettävä toimimaan suojassa ja vaikuttamaan vastustajan kriittisiin osiin. Elektroninen sodankäynti luo mahdollisuuden ylivoimaiseen tekniseen suorituskykyyn ja avaa uusia operatiivisia mahdollisuuksia lukumääräisesti ylivoimaisen vastustajan lyömiseen. Jos esimerkiksi vastustaja ei kykene johtamaan hävittäjiään tai sillä ei ole käsitystä tilanteesta, lukumääräisesti vähäisilläkin torjuntahävittäjillä voidaan torjua ylivoimainen vastustaja. Tämä kuitenkin edellyttää rahan kanavoimista myös elektronisen sodankäynnin järjestelmiin, jolloin esimerkiksi torjuntahävittäjiä on vastaavasti varaa hankkia vähemmän. Koska ELSO:n vaikutusta on kuitenkin vaikea mieltää, kiusaus hankkia koko rahalla asejärjestelmiä on kovin suuri. Mutta hieman haasteellisesti voidaan kysyä, onko järkeä hankkia 60 järjestelmää tappiosuhteella 3:1 jos voi hankkia 40 järjestelmää tappiosuhteella 80:1?

# LIITE 1: Sähkömagneettinen spektri

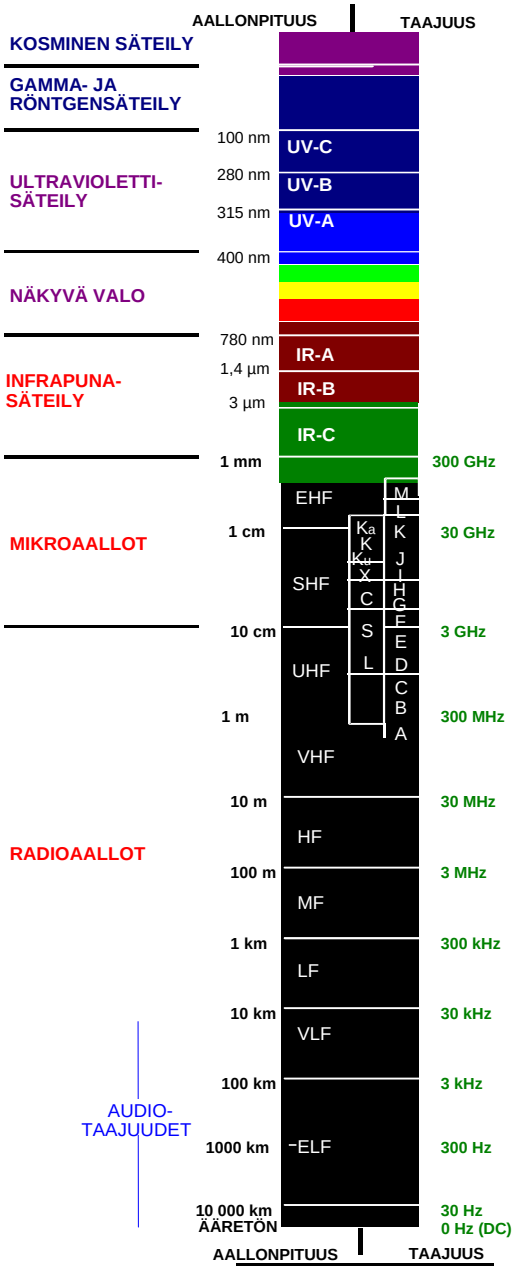
## Radiotaajuinen säteily

Spektrin alapäässä (taajuus hyvin pieni eli aallonpituus hyvin suuri) sijaitsevat radioaallot. Ne jaetaan seuraaviin alueisiin:

ELF (Extremely Low Frequency) 30 – 3000 Hz
VLF (Very Low Frequency) 3 – 30 kHz
LF (Low Frequency) 30 – 300 kHz
MF (Medium Frequency) 0,3 – 3 MHz
HF (High Frequency) 3 – 30 MHz
VHF (Very High Frequency) 30 – 300 MHz
UHF (Ultra High Frequency) 0,3 – 3 GHz

Aaltoalueita on nimetty ajan mittaan sitä mukaa kuin sovelluksia uusille alueille on kehitetty. Tämä näkyy taajuusalueiden hieman keinotekoiselta kuulostavassa nimeämisessä.

***ELF- (30 Hz - 3 kHz) ja VLF-alueita (3 - 30 kHz)*** käytetään lähinnä radionavigointiin sekä meriviestiliikenteeseen signaalien luotettavan etenemisen ja pienen yhteysvälivaimennuksen vuoksi. Suuren aallonpituuden (10 000 – 10 km) vuoksi vaadittavat antennirakenteet ovat hyvin suuria. ***LF-aluetta (30-300 kHz)*** käytetään radionavigointiin sekä meriviestiliikenteeseen. LF-aallot etenevät maanpinta-aaltoina (ground waves), heijastumalla ionosfääristä (sky waves) tai suoraan näköyhteysreittiä pitkin (space waves) mahdollistaen




**Kuva L1.1: Sähkömagneettisen spektrin osat.**

pitkiä yhteyksiä. ***MF-aluetta (300 kHz - 3 MHz)*** käytetään radionavigoinnissa, liikkuvissa (meri- ja ilma-) ja kiinteissä viestiliikennejärjestelmissä, yleisradioiden keskiaaltoradiolähetyksissä sekä horisontin taakse katsovissa tutkajärjestelmissä. MF-aallot etenevät päiväsaikaan maanpinta-aaltoina.

***HF-aluetta (3-30 MHz)*** käytetään muun muassa pitkän kantaman maa-, meri- ja lentoliikenteen viestiliikennetarpeisiin, radioamatöörikäyttöön, radio-astronomiaan sekä yleisradiolähetyksiin (lyhytaaltolähetykset). Pitkän kantaman vuoksi HF-alueella on runsaasti sotilas- ja diplomaattiviestiliikennettä. HF-alue on hyvin ruuhkainen, osin sen vuoksi, että kaukanakin toisistaan sijaitsevat lähetykset häiritsevät toisiaan. HF-aluetta hyödynnetään myös horisontin taakse katsovissa tutkissa. HF-alueella ionosfääristä tapahtuva heijastuminen on primäärinen etenemismuoto, joskin pinta-aaltoa käytetään joissain taktisissa radioissa. Pinta-aallon maksimikantaman ja ionosfääriheijastuksen minimietäisyyden väliin noin 30-60 km etäisyydelle lähettimestä saattaa jäädä kuollut alue, johon ei saada radioyhteyttä. On syytä huomata, että myös länsimaissa HF-alueen merkitys on jälleen nousemassa merkittävämpään asemaan sotilassovelluksissa satelliittitietoliikenteeseen liittyvien häirintäriskien vuoksi.

***VHF-aluetta (30-300 MHz)*** käytetään pääsääntöisesti kiinteän ja liikkuvan tietoliikenteen ja yleisradiotoiminnan tarpeisiin. Lisäksi kaistaa hyödynnetään radio-astronomiassa, radionavigoinnissa sekä tutkakäytössä. VHF-alueella toimivien pitkän kantaman ennakkovaroitustutkien kantama voi olla 1000 km luokkaa korkealla lentäviin maaleihin. Siirtyvä maaradioliikenne, mm. taksit, elinkeinoelämä ja energiahuolto käyttävät alueen alapäätä (75,2 - 87,5 MHz) pienen etenemisvaimennuksen vuoksi. Samasta syystä VHF-kenttäradiot toimivat tyypillisesti 30 ja 88 MHz välisellä kaistalla.

***UHF-aluetta (300 MHz - 3 GHz)*** käytetään kiinteiden ja siirrettävien radiolinkkien tarpeisiin, televisiolähetyksiin, satelliittilinkkeihin, matkapuhelin- ja viranomaisradioverkoissa, langattomissa lähiverkoissa, sekä ennakkovaroitus- ja ilmavalvontatutkissa ja satelliittipaikannusjärjestelmissä. Myös NATO:n taktiset radiolinkit toimivat tällä alueella. UHF-alue on lähes täynnä eli lähestulkoon kaikki taajuudet on allokoitu ja käytössä eri sovelluksissa. UHF-taajuuksilla radioaalto etenee lähes pelkästään näköyhteysreittiä pitkin ja yhteydet rajautuvat lähettimen ja vastaanottimen antennien korkeuksista riippuvaan radiohorisonttiin. Esteet näköyhteysreitillä vaimentavat signaalia voimakkaasti.

SHF- (Super High Frequency) ja EHF-alueiden (Extremely High Frequency) yhteydessä puhutaan yleensä ***mikroaalloista***. EHF-alue ulottuu 300 GHz:iin, jossa aallonpituus on 1 mm.

***SHF-aluetta (3 - 30 GHz)*** käytetään kiinteiden televerkkojen radiolinkeissä (myös joissakin taktisissa radiolinkkijärjestelmissä), radionavigointijärjestelmissä, satelliittilinkeissä sekä erilaisissa lyhyen kantaman langattomissa sovelluksissa, kuten langattomissa lähiverkoissa. Useimmat hyvää erottelukykyä tarvitsevat tutkat, kuten lentokoneiden monitoimitutkat, ilmatorjunnan seurantatutkat, maastonvalvontatutkat,

vastatykistötutkat sekä säätutkat toimivat SHF-alueella. SHF-alueelta alkaen säteilyn aallonpituus on niin pieni, että säteily ei juurikaan heijastu, vaan siroaa osuessaan pinnan epätasaisuuksiin

***EHF-alueella (30 - 300 GHz)*** aallonpituus on millimetriluokkaa, minkä vuoksi alueesta käytetään myös nimitystä ***millimetriaaltoalue***. Hyvin lyhyen aallonpituuden vuoksi järjestelmien komponentit, erityisesti antennit, ovat pieniä, minkä vuoksi millimetriaaltotutkia käytetään hyväksi hakupäissä. Toisaalta suuria lähetystehoja ei saada tuotettua yhtä helposti kuin matalammilla taajuuksilla.

Tutkasovellusten kehittyessä toisen maailmansodan aikana nimettiin tutkatekniikan käyttöä varten omia taajuuskaistoja. Käyttöön ovat jääneet sodan voittaneiden liittoutuneiden käyttämä jako, jossa salaussyistä kaistat nimettiin seuraavanlaisesti:

| nimi | taajuusalue | tyypillisiä esimerkkejä käyttötarkoituksista |
|---|---|---|
| P | 230 MHz – 1 GHz | pitkän kantaman (vanhat, mutta antihäive-)tutkat, kasvillisuutta, jäätä ja maata läpäisevät tutkat |
| L | 1 – 2 GHz | ilma- ja merivalvontatutkat, 2D-valvontatutkat |
| S | 2 – 4 GHz | kohdevalvontatutkat, 3D-valvontatutkat, AWACS |
| C | 4 – 8 GHz | vastatykistötutkat, meteorologiset tutkat |
| X | 8 – 12 GHz | hävittäjätutkat, ilmatorjuntajärjestelmien tulenjohtotutkat, maastonvalvontatutkat |
| Ku | 12 – 18 GHz | maastonvalvontatutkat, tulenjohtotutkat |
| K | 18 – 26,5 GHz | täsmäaseiden millimetriaaltohakupäät |
| Ka | 26,5 – 40 GHz | täsmäaseiden millimetriaaltohakupäät |

NATOssa on vakioitu kaistoille seuraavat nimitykset:

| | | | |
|---|---|---|---|
| A | 0 – 250 MHz | G | 4 – 6 GHz |
| B | 250 – 500 MHz | H | 6 – 8 GHz |
| C | 500 MHz – 1 GHz | I | 8 – 10 GHz |
| D | 1 – 2 GHz | J | 10 – 20 GHz |
| E | 2 – 3 GHz | K | 20 – 40 GHz |
| F | 3 – 4 GHz | L | 40 – 60 GHz |
| | | M | 60 – 100 GHz |

Molemmat edellä kuvatuista tutkataajuuksien nimeämistavoista ovat laajassa käytössä.

## Optinen säteily

Optisen säteilyn alue käsittää infrapunasäteilyn, näkyvän valon ja ultraviolettisäteilyn. ***Infrapunasäteily*** ulottuu millimetrin aallonpituudesta aina näkyvän valon aallonpituudelle asti. Sitä hyödynnetään muun muassa tiedustelujärjestelmissä, maalin-

seuraimissa, lämpötähtäimissä, hakupäissä ja tietoliikenteessä. Alue voidaan jakaa aallonpituuden perusteella ainakin neljällä eri tavalla:

1. IR-A 780-1400 nm
   IR-B 1,4 - 3,0 µm
   IR-C 3 µm - 1 mm

| | | |
|---|---|---|
| 2. NIR, Near Infra-Red | Lähi-infrapuna | 780 nm - 3 µm |
| MIR, Middle Infra-Red | Keski –”– | 3 - 6 µm |
| FIR, Far Infra-Red | Kauko –”– | 6 - 15 µm |
| XIR, eXtreme Infra-Red | Ääri –”– | 15 - 1000 µm |
| 3. NIR, Near Infra-Red | Lähi-infrapuna | 0,7 - 1,1 µm |
| SWIR, Short-Wavelength IR | Lyhytaalto-IP | 1,1 - 3,0 µm |
| MWIR, Medium-Wave IR | Keskiaalto-IP | 3,0 - 5,0 µm |
| LWIR, Long-Wavelength IR | Pitkäaalto-IP | 5,0 - 20 µm |
| 4. Heijastuva infrapuna | | 780 nm - 3,0 µm |
| Terminen infrapuna | | 3,0 - µm |

Nimityksellä ***valo*** tarkoitetaan *ihmisen silmälle näkyvää* säteilyä 400-780 nm alueella.

***Ultraviolettialue*** jaetaan kolmeen alueeseen: UV-A (315 – 400 nm), UV-B (280 – 315 nm) ja UV-C (100 – 280 nm). Aluetta käytetään tiedustelutarkoituksissa erottamaan keinotekoisia kohteita luonnontaustasta, erityisesti lumesta, sekä passiivisissa ohjusvaroittimissa.

# LIITE 2: SUOJAUTUMINEN ELEKTRONISELTA TIEDUSTELULTA JA VALVONNALTA

Vastustajan elektroniselta tiedustelulta ja valvonnalta voidaan suojautua sekä teknisin että toiminnallisin keinoin. Teknisiä keinoja on käsitelty kattavasti MpKK:n Tekniikan laitoksen julkaisussa *Digitaalinen Taistelukenttä*. Seuraavassa käsitellään toiminnallisia keinoja ja yksinkertaisia menetelmiä, joiden avulla voidaan arvioida vastustajan mahdollisuudet havaita oma järjestelmämme. Mikäli tekniikan peruskäsitteet eivät ole lukijalle selviä, häntä kehotetaan lukemaan ensin liite 5.

Tämä liite pyrkii antamaan vastaukset kysymyksiin:

- Millaisin edellytyksin järjestelmä paljastuu vastustajan elektroniselle tiedustelulle?
- Minkälaisin keinoin voidaan vähentää paljastuvuutta vastustajan elektroniselle tiedustelulle?
- Miltä etäisyydeltä erilaisten järjestelmien voidaan olettaa paljastuvan maassa tai ilmassa toimivalle elektronisen tiedustelun järjestelmälle?
- Minkälaisella tarkkuudella vastustajan voidaan olettaa kykenevän paikantamaan havaitsemansa järjestelmät?

Asiat kuvataan liitteessä kuvataan riittävästi yleistettyinä ja suhteellisen karkeiden peukalosääntöjen avulla. Näillä mahdollistetaan nopeiden arvioiden tekeminen ilman vaativia laskutoimituksia. Lukijan toivotaan kuitenkin ymmärtävän, että näin saatavat arviot ovat luonteeltaan vain karkeita, keskimääräisiä ja pätevät yleisellä tasolla.

## Edellytykset elektroniselle tiedustelulle paljastumiselle

Järjestelmän paljastuminen vastustajan elektroniselle tiedustelulle ja valvonnalle edellyttää kaikkien seuraavien seikkojen toteutumista:

1. Tiedustelujärjestelmä kykenee *sieppaamaan* signaalin. Tällöin sen on valvottava oikeaa suuntaa ja taajuutta juuri sillä hetkellä, jona oma järjestelmämme lähettää kyseiseen suuntaan ja kyseiselle taajuudelle.
2. Tiedustelujärjestelmä kykenee *ilmaisemaan* signaalin. Tällöin sen on saatava riittävän pitkäksi aikaa riittävän voimakas signaali vastaanottimelleen kohdan 1 ehdon täyttyessä. Yleensä tiedustelujärjestelmät ovat teknologisesti sillä tasolla, että ne kykenevät ilmaisemaan hyvinkin lyhyet signaalit, joten ilmaisu riippuu lähinnä vastaanottimelle saapuvan signaalin voimakkuudesta.

3. Tiedustelujärjestelmä tai -operaattori kykenee *hyödyntämään* signaalin kohtien 1-2 ehtojen täyttyessä. Vaatimuksista riippuen tämä voi tarkoittaa esimerkiksi yksinkertaista automaattista suuntimista, viestiliikenteen vieraskielisen puheen ymmärtämistä, kohteen tunnistamista tai vaikeimmillaan monimutkaista teknistä tai kryptologista analyysiä.

Tiedustelujärjestelmissä on usein kaksi toisiaan tukevaa osaa:

1. signaalin *sieppaustodennäköisyyden*[t] maksimoimiseksi optimoitu laajaa sektoria ja leveää taajuuskaistaa valvova *hakusuuntimo*[u], jonka tehtävänä on havaita lyhyetkin lähetteet ja suuntia niiden lähetin. Nykyaikainen hakusuuntimo kykenee havaitsemaan käytännössä hyvin lyhyet tai hyppivätaajuisetkin lähetteet jopa 360 asteen sektorista.
2. signaalin *ilmaisutodennäköisyyden* maksimoimiseksi optimoitu hyvin kapeaa sektoria ja yleensä myös suhteellisen kapeaa taajuuskaistaa kerrallaan tarkasteleva *seuranta- ja analysointijärjestelmä*, jonka tehtävänä on kerätä lisää tietoja ja tarkentaa jo kerättyjä tietoja hakusuuntimon antaman osoituksen perusteella.

Ensin mainitun järjestelmän toiminnallinen herkkyys voi olla esimerkiksi -80 dBm:n luokkaa, kun se jälkimmäisessä voi olla esimerkiksi -100 dBm. Tällä tarkoitetaan sitä, että mikäli oman järjestelmämme signaalin voimakkuus tiedustelujärjestelmän kohdalla on yli -80 dBm hakusuuntimon tai -100 dBm analysointivastaanottimen kohdalla sillä hetkellä kun tiedustelujärjestelmä toimii oman järjestelmämme suuntaan, sen voidaan olettaa kykenevän havaitsemaan meidät.

Tiedustelu*järjestelmän* herkkyys muodostuu karkeasti ottaen kahdesta tekijästä:

1. Tiedustelu*vastaanottimen* toiminnallinen herkkyys: kuinka pienitehoisen signaalin vastaanotin ja operaattori kykenee havaitsemaan ja hyödyntämään.
   - Kapeakaistaisen (1 MHz hetkellinen kaista) ***tutka-alueen tiedustelu-vastaanottimen*** herkkyys voi olla esimerkiksi -90 dBm, kun taas laajakaistaisen (500 MHz hetkellinen kaista) vastaanottimen herkkyys voi olla esimerkiksi -63 dBm.
   - Erittäin kapeakaistaisella (25 kHz) ***viestialueen tiedusteluvastaanottimella*** herkkyys voi olla esimerkiksi -106 dBm ja laajakaistaisella (3 MHz) hakuvastaanottimella esimerkiksi -85 dBm.

---

[t] Todennäköisyyskäsitteistä käytetään usein lyhenteitä POI (Probability of Intercept), POD (Probability of Detection) ja POE (Probability of Exploitation; näistä epämääräisin todennäköisyyskäsite). Vastaavasti järjestelmiä, joita on hankala siepata, ilmaista tai hyödyntää, kutsutaan lyhenteillä LPI (Low Probability of Intercept), LPD (Low Probability of Detection) ja LPE (Low Probability of Exploitation). On kuitenkin huomattava, että tämä noudattaa Suomen puolustusvoimien määritelmiä – kansainvälisessä kirjallisuudessa esim. termejä POI ja LPI käytetään usein merkityksessä, joka vastaa suomalaisia POD- ja LPD-termejä.

[u] ELTU-järjestelmässä voi olla myös erilliset haku/seuranta- ja suuntimojärjestelmät.

2. Vastaanottimeen liitetyn antennin vahvistus: kapeakeilaisella antennilla tutka-alueella vahvistus voi olla 24..30 dB:n luokkaa ja viestialueella 20..24 dB luokkaa. Laajaa tilaa valvovien ympärisäteilevien antennien vahvistus on 3 dB:n suuruusluokkaa.

Kokonaisjärjestelmän isotrooppinen herkkyys[v] saadaan vähentämällä vastaanottimen herkkyydestä siihen liitetyn antennin vahvistus. Edellä kuvatut esimerkit ovat vain suuntaa-antavia, sillä todellisten järjestelmien herkkyys riippuu huomattavasti siitä, mikä on järjestelmän käyttötarkoitus (omasuoja, elektroninen tuki, signaalitiedustelu jne.) ja minkälaisiin kompromisseihin erilaisten suorituskyky- ja hintatekijöiden kesken on päädytty.

## Suojautuminen elektroniselta tiedustelulta

Suojautuminen tiedustelulta on mahdollista rikkomalla edellisessä luvussa kuvattu tiedustelujärjestelmän toimintoketju: signaalin sieppaus – signaalin ilmaisu – signaalin hyödyntäminen. Mikäli vastustaja ei kykene sieppaamaan tai ilmaisemaan signaalia, edes järjestelmämme olemassaolo saati sijainti ei paljastu. Jos vastustaja sen sijaan kykenee ilmaisemaan ja sieppaamaan signaalin, järjestelmämme olemassaolo ja sijainti paljastuu, vaikka vastustaja ei muutoin kykenisikään hyödyntämään sieppaamaansa signaalia. Tämän vuoksi paras suoja tiedustelulta saavutetaan estämällä joko sieppaus tai ilmaisu. Molempia ei tarvitse estää.

Sieppaustodennäköisyyden minimoimisen tavoitteena on antaa vastustajalle mahdollisuus signaalin sieppaamiseen mahdollisimman harvoin ja mahdollisimman lyhyeksi aikaa. Se voidaan toteuttaa esimerkiksi seuraavin tavoin:

1. Käytetään niin pientä lähetystehoa, ettei vastustaja voi käyttää joka suuntaan tai laajaan sektoriin havainnoivia ympärisäteileviä antenneja, vaan se pakotetaan käyttämään voimakkaasti suuntaavia antenneja, jotka voivat valvoa vain yhtä suuntaa kerrallaan.
2. Käytetään voimakkaasti suuntaavia (matalasivukeilaisia) antenneja siten, että antennin pääkeila osoittaa mahdollisimman harvoin ja lyhyen aikaa kerrallaan kohti vastustajaa.
3. Käytetään niin nopeaa ja laajakaistaista taajuushypytystä, että se estää vastustajaa seuraamasta lähetettämme jatkuvasti.

[v] Isotrooppinen herkkyys kuvaa tiedustelujärjestelmän antennivahvistuksen ja vastaanottimen herkkyyden yhteisvaikutusta, siis kokonaisjärjestelmän kykyä havaita heikkoja signaaleja, ja se lasketaan vähentämällä vastaanottimen herkkyydestä antennivahvistuksen arvo. Jos siis vastaanottimen herkkyys on esim. -60 dBm ja tiedustelujärjestelmän antennivahvistus 10 dB, on tiedustelujärjestelmän isotrooppinen herkkyys -70 dBm.

Ilmaisutodennäköisyyden minimoimisen tavoitteena on mahdollisimman pienen tehon säteileminen vastustajan suuntaan tai vastustajan tiedustelujärjestelmän herkkyyden huonontaminen. Tämä on mahdollista esimerkiksi seuraavin keinoin:

1. Käytetään mahdollisimman pientä lähetystehoa, mieluiten niin pientä tehoa, että järjestelmä juuri ja juuri toimii[w].
2. Käytetään voimakkaasti suuntaavia antenneja (poispäin tiedustelu-järjestelmästä) sekä antenneja, joiden sivukeilataso on mahdollisimman pieni.
3. Suunnitellaan järjestelmän sijoitus ja käyttö siten, että suuntaavien antennien pää- ja takakeilat sekä suurimmat sivukeilat eivät suuntaudu vastustajaan päin ja käytetään tutkajärjestelmissä lähettimen sammutusta antennin osoittaessa uhkasuuntiin.
4. Sijoitetaan omat asemat siten, että vastustajan suuntaan on maastoeste.
5. Pakotetaan vastustaja toimimaan laajalla taajuuskaistalla (vastaanottimen herkkyys huononee) esim. käyttämällä taajuushypytystä ja hankitaan omat järjestelmät kattamaan hyvin laaja kokonaistaajuusalue.
6. Nostetaan vastustajan tiedustelujärjestelmän (ulkoista) kohinatasoa lähettämällä vastustajan tiedustelujärjestelmää kohti häiritsevää signaalia.

Oma signaali voidaan myös peittää käyttämällä samanaikaisesti useita samanlaisia lähettimiä, jolloin signaali peittyy jossain määrin muiden lähetteiden joukkoon, tai käyttämällä aktiivisia häirintälähettimiä.

Vastustajan tiedustelujärjestelmän sieppaamaan ja ilmaiseman signaalin hyödyntämistä voidaan vaikeuttaa salaamalla lähete, muuttamalla lähetysparametreja sekä käyttämällä vaikeasti tulkittavia lähetteitä. Tällä ei pyritä estämään järjestelmän paljastumista, vaan vaikeutetaan vastustajan tiedustelun tulkinta- ja analysointiprosessia ja siten hidastetaan johtopäätösten tekemistä ja viivästetään vastatoimenpiteitä – eli minimoidaan signaalin hyödyntämisen todennäköisyys.

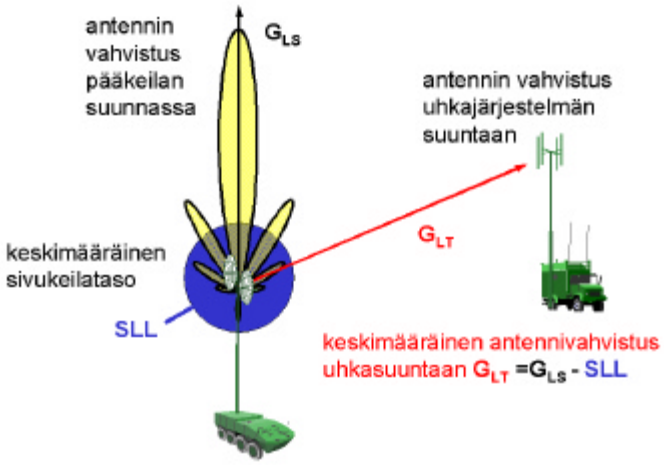
## Paljastumisetäisyyden määrittäminen

Järjestelmän paljastumisetäisyys voidaan karkeasti arvioida, kun tiedetään seuraavat tekniset parametrit:

- oman järjestelmän lähetysteho
- oman järjestelmän antennivahvistus uhkasuuntaan (katso kuva L2.1)

[w] Tiedustelujärjestelmä havaitsee oman järjestelmämme yksittäisellä taajuudella lähetetyn huipputehon perusteella, kun taas oman järjestelmämme toiminta perustuu kokonaistehon tai tutkassa pulssin energian havainnointiin. Mikäli siis voimme levittää lähetettä spektrissä tai ajassa, sen huipputeho pienenee ilman että oma toiminta oleellisesti kärsii. Tähän perustuvat suorahajotushajaspektriviestijärjestelmien tai tutkajärjestelmien, joissa on hyvin pitkät pulssit tai jopa jatkuva lähete, vaikea havaittavuus.

- vastustajan tiedustelujärjestelmän etäisyys ja toimintakorkeus
- arvio vastustajan tiedustelujärjestelmän isotrooppisesta herkkyydestä (tai tiedusteluvastaanottimen herkkyydestä ja järjestelmän antennivahvistuksesta).




**Kuva L2.1: Jos tiedustelu-uhka ei kohdistu järjestelmään sen pääkeilasta, on arvioitava järjestelmän antennivahvistus uhkasuuntaan. Mikäli tätä ei voi määrittää tarkasti antennin keilakuviosta, lasketaan yleensä keskimääräinen antennivahvistus uhkasuuntaan vähentämällä pääkeilan antennivahvistuksesta sivukeilataso, joka kuvaa kuinka paljon pääkeilaa pienempi järjestelmän antennivahvistus pääkeilan ulkopuolella keskimäärin on.**

Järjestelmän lähetysteho ja antennivahvistus uhkasuuntaan muodostavat signaalin lähtötason järjestelmän kohdalla. Kun signaali etenee kauemmas järjestelmästä, se vaimenee. Vaimennus riippuu muun muassa lähetteen taajuudesta, välillä olevista esteistä ja maastosta sekä siitä, onko vastaanotin ”näköyhteydellä”[x] lähettimestä eli käytännössä radiohorisontin sisäpuolella. Radiohorisontin karkea etäisyys voidaan laskea kaavalla

$$R_{RH} = 4{,}1 \cdot \sqrt{h_L} + 4{,}1 \cdot \sqrt{h_T}$$

missä $R_{RH}$ on radiohorisontin etäisyys kilometreinä, $h_L$ oman lähettimemme ja $h_T$ tiedusteluvastaanottimen korkeus metreinä. Tämä tarkoittaa siis sitä maksimiyhteysväliä, jolla tiedustelija ei jää radiohorisontin taakse. Taulukossa L2.1 on kuvattu radiohorisontin etäisyys erilaisilla antennikorkeuksilla.

[x] Todellisuudessa radiohorisontti on noin 10% optista horisonttia kauempana.

| | 0 m | 10 m | 20 m | 50 m | 100 m | 200 m | 500 m | 1 km | 2 km | 10 km | 20 km |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 m | 0 | 13 | 18 | 29 | 41 | 58 | 92 | 130 | 183 | 410 | 580 |
| 10 m | 13 | 26 | 31 | 42 | 54 | 71 | 105 | 143 | 196 | 423 | 593 |
| 20 m | 18 | 31 | 37 | 47 | 59 | 76 | 110 | 148 | 202 | 428 | 598 |
| 50 m | 29 | 42 | 47 | 58 | 70 | 87 | 121 | 159 | 212 | 439 | 609 |
| 100 m | 41 | 54 | 59 | 70 | 82 | 99 | 133 | 171 | 224 | 451 | 621 |
| 200 m | 58 | 71 | 76 | 87 | 99 | 116 | 150 | 188 | 241 | 468 | 638 |
| 500 m | 92 | 105 | 110 | 121 | 133 | 150 | 183 | 221 | 275 | 502 | 672 |
| 1 km | 130 | 143 | 148 | 159 | 171 | 188 | 221 | 259 | 313 | 540 | 709 |
| 2 km | 183 | 196 | 202 | 212 | 224 | 241 | 275 | 313 | 367 | 593 | 763 |
| 10 km | 410 | 423 | 428 | 439 | 451 | 468 | 502 | 540 | 593 | 820 | 990 |
| 20 km | 580 | 593 | 598 | 609 | 621 | 638 | 672 | 709 | 763 | 990 | 1160 |

**Taulukko L2.1: Radiohorisontin etäisyys kilometreinä eri antennikorkeuksilla eli maksimiyhteysväli kahden eri korkuisen antennin välillä siten, ettei vastaanotto-antenni jää radiohorisontin taakse.**

Mikäli tiedusteluvastaanotin on radiohorisontin sisäpuolella eikä välillä ole esteitä, voidaan vaimennus laskea ns. vapaan tilan vaimennuksen kaavalla *desibeleinä*:

$$L_V = 32{,}4\,\mathrm{dB} + 20 \cdot \log_{10}(R_{km}) + 20 \cdot \log_{10}(f_{MHz})$$

missä $L_V$ on vapaan tilan vaimennus desibeleinä, $R$ yhteysvälin pituus kilometreinä ja $f_{MHz}$ lähetteen taajuus megahertseinä[y]. Taulukossa L2.2 on listattu vapaan tilan vaimennuksen numeroarvoja joillakin eri etäisyyksillä ja lähetystaajuuksilla. Peukalosääntöinä voi painaa mieleen jonkin arvon taulukosta ja huomata, että vaimennus kasvaa 6 dB aina kun etäisyys tai taajuus kaksinkertaistuu.

Mikäli tunnetaan oman järjestelmän lähetysteho, antennivahvistus tiedustelu-järjestelmän suuntaan ja yhteysvälivaimennus, voidaan oman signaalin voimakkuus tiedustelujärjestelmän kohdalla laskea *desibeleinä* seuraavasti:

$$P_T = P_L + G_L - L$$

missä $P_T$ on oman signaalimme teho tiedustelujärjestelmän kohdalla, $P_L$ oman järjestelmämme lähetysteho (esim. yksiköissä dBm) ja $G_L$ oman järjestelmämme

[y] Vapaan tilan vaimennuksen kaava on hieman harhaanjohtava ja sitä voi käyttää ainoastaan tässä kuvatussa laskennassa, koska siihen on huomioitu myös yhteyteen liittyvän järjestelmän antennin ominaisuuksia (vahvistuksen taajuusriippuvuutta), ei ainoastaan radioaaltojen vaimenemista avaruudessa. Signaali vaimenee todellisuudessa edetessään vapaassa tilassa täysin taajuudesta riippumatta, mutta vastaanottoantennin kyky siepata tätä signaalia riippuu taajuudesta. Vapaan tilan vaimennuksen kaava on kuitenkin vakiintunut yleiseen käyttöön ja se yksinkertaistaa muita laskentakaavoja.

antennivahvistus tiedustelijan suuntaan. $L$ on yhteysvälivaimennus, vapaan tilan vaimennuksen tapauksessa edellä mainittu $L_V$.

| | 50MHz | 100 M | 200 M | 500 M | 1 GHz | 2 GHz | 5 G | 10 G | 20 G | 50 G | 100 G |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 km | 66 | 72 | 78 | 86 | 92 | 98 | 106 | 112 | 118 | 126 | 132 |
| 2 km | 72 | 78 | 84 | 92 | 98 | 104 | 112 | 118 | 124 | 132 | 138 |
| 5 km | 80 | 86 | 92 | 100 | 106 | 112 | 120 | 126 | 132 | 140 | 146 |
| 10 km | 86 | 92 | 98 | 106 | 112 | 118 | 126 | 132 | 138 | 146 | 152 |
| 20 km | 92 | 98 | 104 | 112 | 118 | 124 | 132 | 138 | 144 | 152 | 158 |
| 50 km | 100 | 106 | 112 | 120 | 126 | 132 | 140 | 146 | 152 | 160 | 166 |
| 100 km | 106 | 112 | 118 | 126 | 132 | 138 | 146 | 152 | 158 | 166 | 172 |
| 200 km | 112 | 118 | 124 | 132 | 138 | 144 | 152 | 158 | 164 | 172 | 178 |
| 500 km | 120 | 126 | 132 | 140 | 146 | 152 | 160 | 166 | 172 | 180 | 186 |
| 1000 km | 126 | 132 | 138 | 146 | 152 | 158 | 166 | 172 | 178 | 186 | 192 |

**Taulukko L2.2: Vapaan tilan vaimennuksen suuruus desibeleinä eri yhteys-etäisyyksillä ja lähetystaajuuksilla. Taajuuden tai etäisyyden kaksinkertaistuminen lisää aina vapaan tilan vaimennusta 6 dB.**

Näiden kaavojen ja taulukoiden avulla voidaan laskea signaalimme taso vastustajan tiedustelujärjestelmän kohdalla. Signaalitasoa verrataan tiedustelujärjestelmän isotrooppiseen herkkyyteen eli tehotasoon, jonka ylittävä signaali voidaan tiedustella. Jos signaalimme on sitä pienempi, sitä ei *todennäköisesti - ja useimmissa tilanteissa* - voida tiedustelujärjestelmällä havaita.

Taulukossa L2.3 on esitetty joitakin esimerkinomaisia, mutta suuruusluokaltaan realistisia, lähettimien ominaisuuksia ja niiden tiedusteluun vaadittavia isotrooppisia herkkyyksiä vapaan tilan vaimenemisen tapauksessa. Tiedusteluvastaanottimien herkkyydet vaihtelevat esim. välillä -40..-105 dBm (yksinkertaisista hyvin laajakaistaisista hienostuneempiin ja erittäin kapeakaistaisiin). Herkkyys voi vielä parantua näistä arvoista (siis vaadittavan signaalin taso pienentyä) jopa n. 30 dB, jos tiedustelujärjestelmä on varustettu voimakkaasti suuntaavalla tiedusteluantennilla. Taulukon avulla voidaan arvioida tiedustelun ulottuvuutta.

Tiedusteluvastaanottimen herkkyys riippuu valitusta vastaanotintekniikasta, mutta erityisesti järjestelmän käyttämästä kaistanleveydestä: jos esim. viestitaajuusalueen tiedusteluvastaanotin pakotetaan siirtymään yksittäisen 4 kHz:n audiokanavan tiedustelusta hyppivätaajuisen radion koko 30 MHz:n kaistan laajakaistaiseen seurantaan, järjestelmän herkkyys heikkenee (herkkyyden lukuarvo kasvaa) vastaavassa suhteessa kuin valvottava taajuusalue laajenee. Tässä tapauksessa heikennys herkkyyteen on lähes 40 dB eli vastaanottimen on saatava lähes 10 000-kertainen signaali kapeakaistaiseen tapaukseen verrattuna! Vastaava pätee tietysti myös tutkataajuuksilla. On siis ensiarvoisen tärkeää toimia siten, että vastustaja joutuu tiedustelemaan mahdollisimman laajakaistaisesti.

| | 5 km | 10 km | 20 km | 50 km | 100 km | 200 km | 500 km |
|---|---|---|---|---|---|---|---|
| Kenttäradio marssiantennilla ($f$=50 MHz, $P_L$=5 W, $G$=0 dB) | -43 | -49 | -55 | -63 | -69 | -75 | -83 |
| Toinen kenttäradio pitkälanka-ant. ($f$=50 MHz, $P_L$=30 W, $G$=8 dB) | -28 | -34 | -40 | -48 | -54 | -60 | -68 |
| Lentokoneradio ($f$=300 MHz, $P_L$= 20 W, $G$=2 dB) | -51 | -57 | -63 | -71 | -77 | -83 | -91 |
| Kenttälinkkijärjestelmä ($f$=800 MHz, $P_L$=10 W, $G$=15 dB) | -49 | -55 | -61 | -69 | -75 | -81 | -89 |
| GSM-puhelin ($f$=1800 MHz, $P_L$=1 W, $G$=2 dB) | -79 | -86 | -92 | -99 | -106 | -112 | -119 |
| Suuri ilmavalvontatutka ($f$=3 GHz, $P_L$=2 MW, $G$=40 dB) | 17 | 11 | 5 | -3 | -9 | -15 | -23 |
| Pieni ilmavalvontatutka ($f$=5 GHz, $P_L$=20 kW, $G$=25 dB) | -22 | -28 | -34 | -42 | -48 | -54 | -62 |
| Mikroaaltolinkki ($f$=8 GHz, $P_L$=0,1 W, G=35 dB) | -69 | -75 | -81 | -89 | -95 | -101 | -109 |
| Hävittäjätutka ($f$=10 GHz, $P_L$=10 kW, $G$=30 dB) | -26 | -32 | -38 | -46 | -52 | -58 | -66 |
| Maastonvalvontatutka ($f$=15 GHz, $P_L$= 10 W, $G$=30 dB) | -60 | -66 | -72 | -80 | -86 | -92 | -100 |

**Taulukko L2.3: Esimerkkejä signaalin voimakkuudesta dBm-yksiköissä tiedustelujärjestelmän kohdalla joidenkin tyypillisten johtamis- ja valvonta-järjestelmien tapauksessa, *tiedusteltaessa pääkeilan suunnasta*. Sivukeilasta tiedusteltaessa luvuista pitää vielä vähentää pääkeilan ja sivukeilan vahvistusten erotus, tyypillisesti noin 20 dB. Luvut kuvaavat sitä isotrooppista herkkyyttä, mikä tiedustelujärjestelmältä vaaditaan kyseisten järjestelmien tiedusteluun. Taulukossa oletetaan signaalin etenevän vapaassa tilassa.**

Vaikka vastustajan on mahdollista saada tiedustelujärjestelmänsä herkkyys erittäin hyväksi toimimalla kapeakaistaisella vastaanottimella ja suuren vahvistuksen antennilla, ei tämän pidä antaa lannistaa: kapeakaistaisuus ja voimakkaasti suuntaava antenni estävät jatkuvan valvonnan kaikkiin suuntiin ja kaikilla taajuuksilla, mikä pienentää sieppaustodennäköisyyttä ja siten aiheuttaa vastustajalle suuria ongelmia taktisessa tilanteessa, jossa tiedusteluun kuluvalla ajalla on merkitystä. Kyseessä onkin tiedustelijan optimointiongelma: pyrkiäkö mahdollisimman suureen tiedustelu-etäisyyteen vai reaaliaikaisuuteen ja jatkuvaan valvontaan.

## Esimerkki L2.1

Tarkastellaan kenttälinkin paljastuvuutta vastustajan ***ilmasta*** suorittamalle elektroniselle tiedustelulle. Arviointi suoritetaan taulukoiden avulla seuraavasti:

1. Arvioidaan tiedustelujärjestelmän herkkyys. Oletetaan tarkasteltavassa tilanteessa uhkana olevan laajakaistainen tiedusteluvastaanotin, jonka herkkyydeksi on aiemmin esitetty -85 dBm. Oletetaan, että tiedustelu-järjestelmä valvoo laajaa sektoria, jolloin sen antennivahvistus on 3 dB. Tiedustelujärjestelmän isotrooppinen herkkyys on siis:

-85 dBm - 3 dB = -88 dBm

2. Arvioidaan tiedustelujärjestelmän toimintakorkeus ja määritetään kuinka kaukana radiohorisontti on. Jos tiedustelujärjestelmän arvioidaan lentävän 10 kilometrin korkeudessa ja tarkastelevan linkkiantennia, joka on asennettu 20 metrin mastoon ja sijoitettu 30 metrin mäelle (antennikorkeus yhteensä 50 m), saadaan taulukosta L2.1 radiohorisontin etäisyydeksi 439 km. Tiedustelujärjestelmä näkee siis reilun 400 kilometrin päähän, mikäli se on tarpeeksi herkkä ja signaali riittävän voimakas.

3. Katsotaan taulukosta L2.3 kuinka kaukana kenttälinkin signaali ylittää tiedustelujärjestelmän herkkyyden eli on yli -88 dBm. Taulukosta voidaan todeta, että pääkeilan suunnassa linkki on pääkeilastaan tiedusteltavissa herkkyytensä puolesta noin 500 kilometrin päästä.

4. Todetaan, että pääkeilassa radiohorisontti rajaa tiedusteluetäisyyden, joka on nelisensataa kilometriä, joten radiolinkki paljastuu pääkeilastaan 400 km päähän.

5. Arvioidaan mikä on järjestelmän paljastuvuus, jos tiedustelujärjestelmä ei saa pääkeilaa kiinni eli tiedustelukone ei lennä pääkeilan osoittaman suunnan ylitse. Arvioidaan järjestelmän sivukeilatasoksi 20 dB, joka vähennetään järjestelmän tehotasoista (taulukon L2.3 arvoista). Todetaan, että järjestelmän signaalitaso on -69 dBm - 20 dB = -89 dBm 50 km etäisyydellä linkistä. Tämä tehotaso on niin lähellä tiedustelujärjestelmän oletettua herkkyyttä, että voidaan todeta linkin paljastuvan sivukeiloistaan tiedustelukoneelle, joka lentää maksimissaan 50 km etäisyydellä.

Jos taulukot eivät anna suoraan jotakin tietoa, niiden antamia arvoja on helppo muuttaa. Jos edellä esitetyn esimerkin linkki ei toimisikaan 10 watin teholla, kuten taulukko L2.3 olettaa, vaan vaikkapa yhden watin lähetysteholla, vähennetään taulukossa oleva teho (10 W vastaa 40 dBm) ja lisätään uusi teho (1 W vastaa 30 dBm, katso desibeliyksiköiden perusteet liitteestä 5) eli tässä tapauksessa taulukon antamista tehotasoista vähennetään (40-30) = 10. Tällöin 50 kilometrin etäisyydellä linkin tehotaso sivukeilassa olisikin -99 dBm, jota em. järjestelmä ei havaitsisi. 20 km etäisyydellä tiedusteluvastaanottimen saama signaali sivukeilasta olisi -61 dBm - sivukeilataso 20 dB - 10 dB pienempi lähetysteho = -91 dBm, joka on alle tiedusteluvastaanottimen herkkyyden -88 dBm. Toisaalta 10 kilometrin päässä signaaliteho tiedusteluvastaanottimessa olisi -55 - 20 - 10 = -85 dBm, joka ylittää tiedustelun herkkyyden. Tässä tapauksessa linkki siis paljastuisi 10-20 km etäisyydeltä.

Edellä kuvattu esimerkki voidaan myös laskea kaavoilla, jos taulukoita ei haluta käyttää tai mikäli niissä ei ole käytettäväksi soveltuvia arvoja. Tällöin toimitaan seuraavasti:

1. Arvioidaan tiedustelujärjestelmän herkkyydeksi -88 dBm, kuten edellä.

2. Tarkastetaan radiohorisontin kaavalla, onko yhteys radiohorisontin sisällä. Mikäli tilanteessa linkkiantenni on asennettu 20 metrin mastoon ja sijoitettu 30 metrin mäelle ($h_L$=50) ja tiedustelujärjestelmän arvioidaan lentävän 10 kilometrin korkeudessa ($h_T$=10 000), saadaan radiohorisontiksi

$$R_{RH} = 4{,}1 \times v50 + 4{,}1 \times v10000$$
$$= 439 \text{ km}$$

3. Lasketaan linkin lähetysteho eri etäisyyksillä kaavalla $P_T = P_L + G_L - L$
   - esimerkissä on annettu taulukon L2.3 mukaisesti:

     $P_L$ = 10 W = 10 x $\log_{10}(10)$ = 10 dBW = 10 + 30 dBm
     = 40 dBm

     $G_L$ = 15 dB

   Kohdan 2 mukaisesti oletetaan vapaan tilan etenemisvaimennuksen pätevän, jolloin etenemisvaimennus saadaan kaavasta

   $$L_V = 32{,}4 \text{ dB} + 20 \times \log_{10}(R_{km}) + 20 \times \log_{10}(f_{MHz}),$$

   missä linkin taajuus megahertseinä on $f_{MHz}$ = 800. Selvitetään, havaitseeko tiedustelujärjestelmä linkin 50 kilometrin etäisyydeltä, jolloin $R_{km}$ = 50. Tällöin etenemisvaimennukseksi saadaan

   $$L_V = 32{,}4 + 20 \times \log_{10}(50) + 20 \times \log_{10}(800)$$
   $$= 32{,}4 + 34{,}0 + 58{,}1$$
   $$= 125 \text{ dB}$$

   Signaalitasoksi saadaan siten 40 dBm + 15 dB - 125 = -70 dBm.

4. Todetaan johtopäätöksenä, että linkin tehotaso ylittää tiedustelu-vastaanottimen herkkyyden, minkä vuoksi linkki paljastuu pääkeilassa tiedustelulle kyseiseltä etäisyydeltä.

Tarkastelua voidaan jatkaa erilaisin variaatioin. Yleensä kaksi keskeisintä kysymystä ovat:

1. Muuttaako linkin lähetystehon pienentäminen tilannetta olennaisesti?

   Jos lähetystehoa pudotetaan esimerkiksi yhteen wattiin, tiedustelu-etäisyys pienenee kolmannekseen eli taulukon L2.3 mukaan sadan ja kahdensadan kilometrin väliin. Riippuu tilanteesta, onko tällä olennaista merkitystä.

2. Onko linkki havaittavissa myös sivukeiloista?

   Jos linkin sivukeilatasoksi oletetaan vaikkapa 20 dB, tiedustelu-vastaanottimen suuntaan sivukeilassa lähtevä teho pienenee 20 dB eli sadasosaan siitä mikä teho on pääkeilan suunnassa. Taulukon L2.3

tehotasoista on siis vähennettävä 20 dB. Tällöin -88 dBm ylittyy 50 kilometrin päässä.

Edellä esitetyistä kaavoista voidaan johtaa tiedusteluetäisyys vapaan tilan vaimenemisen tapauksessa:

$$R_{km} = \frac{0{,}0239}{f_{MHz}} \cdot 10^{\frac{P_L + G_L - P_T}{20}}$$

missä $R_{km}$ on tiedusteluetäisyys (km), $f_{MHz}$ lähetteen taajuus (MHz), $P_L$ oman järjestelmämme lähetysteho (dBm), $G_L$ oman järjestelmämme antennivahvistus tiedustelijan suuntaan (dB) ja $P_T$ tiedustelujärjestelmän isotrooppinen herkkyys (dBm; eli aiempaan kaavaan suhteutettuna signaalimme teho sen tiedustelujärjestelmän kohdalla, mikä on maksimitiedusteluetäisyyden päässä).

Mikäli tiedusteluvastaanotin ei ole ”näköyhteydellä” lähettimeen eli vapaassa tilassa, vaimennus riippuu voimakkaasti välillä olevista esteistä ja maaston ominaisuuksista. Tämän vuoksi yhteysvälivaimennuksen laskeminen on huomattavasti vaikeampi ja monitahoisempi ongelma kuin vapaan tilan tapauksessa. Yksi suhteellisen moneen tilanteeseen sopiva, mutta vain suuntaa-antava vaimennuksen kaava on ns. Eglin malli, jonka mukaan vaimennuksen mediaani[z] *desibeleinä* on seuraavan kaavan mukainen:

$$L_E = \begin{cases} 85{,}9 + 20 \cdot \log_{10}(f) + 40 \cdot \log_{10}(R) - 20 \cdot \log_{10}(h_L \cdot h_T) & \text{kun } h_T > 10\,\text{m} \\ 76{,}3 + 20 \cdot \log_{10}(f) + 40 \cdot \log_{10}(R) - 20 \cdot \log_{10}(h_L) - 10 \cdot \log_{10}(h_T) & \text{muulloin} \end{cases}$$

missä $f$ on lähetystaajuus megahertseinä, $R$ yhteysvälin etäisyys kilometreinä, $h_L$ lähetysantennin korkeus metreinä ja $h_T$ tiedusteluantennin korkeus metreinä. Etenemisvaimennusmallien käytön yhteydessä on muistettava varmistaa, että malli pätee vain tietyllä parametrialueella. Esimerkiksi Eglin mallin tärkeimmät rajoitukset ovat sen soveltuvuus käytettäväksi vain 30-1000 MHz taajuusalueella ja 1-80 km yhteysväleillä. Alle kilometrin yhteysvälillä malli antaa sitä virheellisempiä arvoja mitä lyhyempi yhteisväli on. Taulukossa L2.4 on kuvattu Eglin mallin mukaisia vaimennuksia esimerkkitilanteissa. Mallia käytetään tyypillisesti tilanteissa, joissa ainakin toinen antenni on suhteellisen matalalla.

Käyttämällä Eglin mallin antamia arvoja aiemmissa kaavoissa tai vertaamalla taulukkoja L2.2 ja L2.4, voidaan arvioida maaston vaikutusta tiedusteluetäisyyteen, ja huomioida näitä arvoja arvioitaessa tiedustelulta ja valvonnalta suojautumista.

[z] Mediaani tarkoittaa, että puolet todellisista vaimennuksista on alle saadun arvon, puolet yli. Sitä miten paljon vaihtelua on eli kuinka paljon tiedusteluetäisyys voi vaihdella olosuhteiden mukaan, ei tällaisista kaavoista näe.

| $R$ | $h_L$ | $h_T$ | 30 MHz | 50 M | 100 M | 200 M | 500 M | 800 M |
|---|---|---|---|---|---|---|---|---|
| 1 km | 1 m | 1 m | 106 | 110 | 116 | 122 | 130 | 134 |
| | 1 | 10 | 96 | 100 | 106 | 112 | 120 | 124 |
| | 10 | 100 | 55 | 60 | 66 | 72 | 80 | 84 |
| 5 | 1 | 1 | 134 | 138 | 144 | 150 | 158 | 162 |
| | 1 | 10 | 124 | 128 | 134 | 140 | 148 | 152 |
| | 10 | 100 | 83 | 88 | 94 | 100 | 108 | 112 |
| 10 | 1 | 1 | 146 | 150 | 156 | 162 | 170 | 174 |
| | 1 | 10 | 136 | 140 | 146 | 152 | 160 | 164 |
| | 10 | 100 | 95 | 100 | 106 | 112 | 120 | 124 |
| 50 | 1 | 1 | 174 | 178 | 184 | 190 | 198 | 202 |
| | 1 | 10 | 164 | 168 | 174 | 180 | 188 | 192 |
| | 100 | 100 | 123 | 128 | 134 | 140 | 148 | 152 |
| 80 | 1 | 1 | 182 | 186 | 192 | 198 | 206 | 210 |
| | 1 | 10 | 172 | 176 | 182 | 188 | 196 | 200 |
| | 10 | 100 | 132 | 136 | 142 | 148 | 156 | 160 |

**Taulukko L2.4: Eglin mallin mukaisia vaimennuksia desibeleinä eri yhteysetäisyyksille ($R$), antennikorkeuksille ($h_L$ ja $h_T$) ja lähetystaajuuksille (30-800 MHz).**

## Esimerkki L2.2

Tarkastellaan kenttäradion ($f$=50 MHz, $P_L$=5 W, $G$=0 dB) paljastuvuutta vastustajan ***pinnasta*** suorittamalle elektroniselle tiedustelulle. Koska käytetty yhteysvälivaimennuksen malli riippuu monesta eri tekijästä ja taulukko L2.4 antaa ainoastaan mielikuvia vaimennuksen suuruudesta muutamassa eri tilanteessa, kuvataan tässä tiedusteltavuuden arviointi laskukaavoja käyttäen:

1. Arvioidaan tiedustelujärjestelmän herkkyys. Oletetaan tarkasteltavassa taktisessa tilanteessa uhkana olevan kapeakaistainen tiedustelu-vastaanotin, jonka herkkyydeksi on aiemmin esitetty -106 dBm. Oletetaan, että tiedustelujärjestelmä valvoo sektoria suuntaavalla antennilla, jolloin sen antennivahvistus on 20 dB. Tiedustelu-järjestelmän isotrooppinen herkkyys on siis:

   -106 dBm - 20 dB = -126 dBm.

2. Koska toimitaan lähellä maanpintaa, radioaaltojen eteneminen ei tapahdu vapaassa tilassa. Pelkästään taulukoita L2.2 ja L2.3 ei siten voi käyttää.

3. Lasketaan linkin lähettämän signaalin tehotaso eri etäisyyksillä kaavalla

   $P_T = P_L + G_L - L$

   - Esimerkissä on annettu $P_L$ = 5 W = 10 x $\log_{10}(5)$

     = 7 dBW = 7 + 30 dBm = 37 dBm

- Esimerkissä $G_L$ = 0 dB
- Koska yhteys ei ole vapaassa tilassa ja Eglin mallin reuna-ehdot ovat voimassa, lasketaan yhteysvälivaimennuksen arvio Eglin mallin mukaisesti. Selvitetään, havaitseeko tiedustelu-järjestelmä lähettimemme 50 km:n etäisyydeltä 10 m:n korkeudessa olevalla antennilla. Tällöin em. Eglin mallin kaavasta saadaan (käytetään kaavan alempaa ”haaraa”, koska tiedusteluantennin korkeus ei ole yli kymmentä metriä):

  $$L = L_E = 76{,}3 + 20 \times \log_{10}(50) + 40 \times \log_{10}(50) - 20 \times \log_{10}(1) - 10 \times \log_{10}(10) = 168 \text{ dB}$$

- Signaalitasoksi tiedustelujärjestelmän kohdalla saadaan siten $P_T$ = 37 dBm + 0 dB – 168 dB = -131 dBm

4. Todetaan johtopäätöksenä, että signaalitaso tiedusteluvastaanottimen kohdalla on tiedustelujärjestelmän isotrooppista herkkyyttä pienempi (-131 dBm < -126 dBm) eli ensimmäisenä johtopäätöksenä voitaisiin todeta oltavan tiedusteluetäisyyden ulkopuolella. Tehoarvojen ero on kuitenkin suhteellisen pieni (5 dB). Tällainen ero voi helposti syntyä väärin arvioidusta vastustajan tiedustelujärjestelmän herkkyydestä ja antennivahvistuksesta, tiedustelijan antennikorkeudesta tai maaston korkeudesta. Lisäksi Eglin vaimenemismalli on suhteellisen epätarkka ja kertoo ainoastaan vaimenemisen mediaaniarvon. Tilanteen suhteen pitääkin olla hyvin varovainen: on täysin mahdollista, että vastustaja kykenee tiedustelemaan radiomme, ainakin osan ajasta.

Tarkastelua voidaan jälleen kehittää erilaisin variaatioin, esim. pohtia kenttäradion lähetystehon, suunta-antennin tai sen sivukeilojen merkitystä tiedusteluetäisyyteen. Esim. mikäli kenttäradiossa käytettäisiinkin 8 dB:n pitkälanka-antennia, sen sivukeilataso tiedusteluvastaanottimen suuntaan olisi 15 dB ja lähetysteho pudotettaisiin 1 wattiin, ei koko laskua kannata tehdä uudestaan (yhteysvälivaimeneminen säilyy vakiona), vaan huomioida ainoastaan muuttuneet arvot. Tällöin sivukeilasta tiedusteltaessa:

$P_L = 10 \times \log_{10}(1) = 0 \text{ dBW} = 0 + 30 \text{ dBm} = 30 \text{ dBm}$

$G_L = 8 \text{ dB} - 15 \text{ dB} = -7 \text{ dB}$

$L_E = 168 \text{ dB}$ (ei muuttunut)

$P_T = 30 \text{ dBm} + (-7 \text{ dB}) - 168 \text{ dB} = -145 \text{ dBm}$

Tässä signaalivoimakkuudessa on jo selvä 19 dB:n ero tiedustelujärjestelmän herkkyyteen (-126 dBm) verrattuna, joten voidaan olettaa, ettei tiedustelu-järjestelmä havaitse radiota. Jälleen täytyy kuitenkin muistaa tilanteeseen liittyvät yleistykset ja olettamukset. Parempi varmuus asiasta edellyttäisi tietokonelaskentaa digitaalisen maastokartan avulla.

On ehdottomasti muistettava, että radioaaltojen eteneminen ja tiedustelun ulottuvuus on oleellisesti tässä liitteessä kuvattua monimutkaisempi ilmiömaailma. Tiedustelun ulottuvuusarviot lasketaan ammattimaisesti laskentaohjelmilla, jotka käyttävät maaston

korkeusvaihtelut sisältäviä digitaalikarttoja ja huomioivat erilaiset radioaaltojen etenemismallit. Myös manuaalinen laskenta on mahdollista ulottaa huomattavasti esitettyä yksityiskohtaisemmaksi.

Kenttäolosuhteissa ja pikatilanteissa yksinkertaisistakin malleista voi kuitenkin olla suojautumisen kannalta tyhjää parempaa hyötyä. On siten hyödyllistä muistaa tyypillisiä tiedustelujärjestelmien herkkyyksiä, omien järjestelmien lähetystehoja ja joitakin yhteysvälivaimennuksen suuruusluokkia. Monissa tilanteissa tiedustelu voi kuitenkin olla mahdollista esitettyä huomattavastikin kauempaa[aa], mihin aina tulee varautua. Esitetyillä keinoilla vastustajan tiedustelijan toimintaa voi kuitenkin huomattavasti vaikeuttaa.

## Paikantamistarkkuuden arviointi

Elektronisen tuen sensorit kykenevät määrittämään suunnan, josta niiden havaitsema signaali tulee. Sensori kykenee kuitenkin määrittämään signaalin tulosuunnan vain tietyllä rajallisella tarkkuudella. Suuntimistarkkuus ilmaistaan kulmayksikköinä, joko radiaaneina tai kansantajuisesti asteina.

Suuntimoista saadut suunnat vaihtelevat jonkin tilastollisen jakauman mukaisesti. Suuntimistarkkuus määritellään tämän jakauman jonakin ominaisuutena – esimerkiksi jakauman keskihajontana. Tämä tarkoittaa käytännössä sitä, että esimerkiksi 2/3 saaduista suuntima-arvoista osuu annetun virherajan sisäpuolelle – siis kahdessa mittauksessa kolmesta kohde todellakin on sensorin määrittämässä suunnassa ilmoitetun tarkkuuden rajoissa. On muistettava, että suuntimo kykenee määrittämään signaalin tulosuunnan itse sensoriin. Jos signaali heijastuu esimerkiksi suuntimoaseman ympäristössä olevasta maastosta, rakennuksista, metalliaidasta, voimalinjoista tai muista kohteista, suuntimon määrittämä lähetteen tulosuunta eroaa lähettimen todellisesta suunnasta.

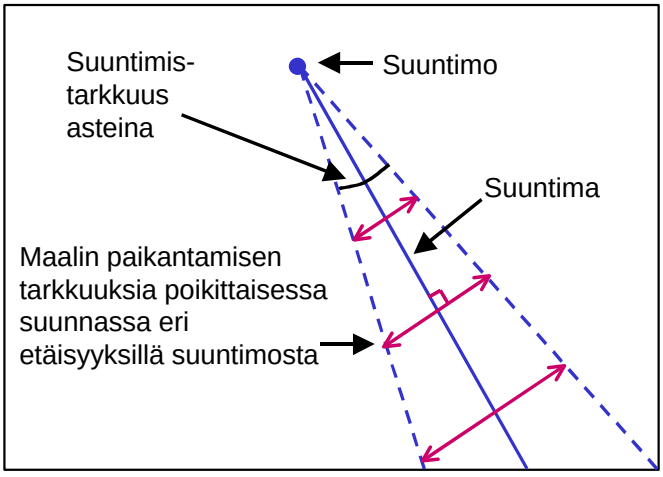
Taulukossa L2.5 on esitetty suuntimistarkkuuksia metreinä ja kilometreinä eri suuntimisetäisyyksillä ja suuntimisen kulmatarkkuuksilla. Luvut tarkoittavat yksinkertaistetusti sitä, kuinka monta metriä lähettimen todellinen paikka voi vaihdella sivusuunnassa suuntimosta katsottuna. Kuva L2.5 esittää poikittaisen tarkkuuden merkityksen lähettimen paikantamisessa.

[aa] HF-taajuuksilla jopa toiselta puolelta maapalloa, sopivissa sääolosuhteissa vesistöjen yllä moninkertaisilta etäisyyksiltä kanavoitumisen vuoksi, hyvin voimakkailla lähetteillä jopa kaukaa radiohorisontin takaa jne.

| | 0,5° | 1° | 2° | 5° | 10° |
|---|---|---|---|---|---|
| 1 km | 9 m | 17 m | 35 m | 87 m | 180 m |
| 2 km | 17 m | 35 m | 70 m | 180 m | 350 m |
| 5 km | 44 m | 87 m | 180 m | 440 m | 880 m |
| 10 km | 87 m | 180 m | 350 m | 870 m | 1,8 km |
| 20 km | 180 m | 350 m | 700 m | 1,7 km | 3,5 km |
| 50 km | 440 m | 870 m | 1,7 km | 4,4 km | 8,7 km |
| 100 km | 870 m | 1,7 km | 3,5 km | 8,7 km | 17 km |
| 200 km | 1,7 km | 3,5 km | 7,0 km | 17 km | 35 km |
| 500 km | 4,4 km | 8,7 km | 17 km | 44 km | 87 km |

**Taulukko L2.5: Paikantamisen poikittainen tarkkuus suuntimosta katsottuna eri suuntimisetäisyyksillä (km) ja suuntimistarkkuuksilla (asteina). Esimerkiksi suuntimistarkkuudella 2° etäisyydellä 50 km oleva kohde on paikannettavissa poikittaissuunnassa 1,7 km tarkkuudella.**

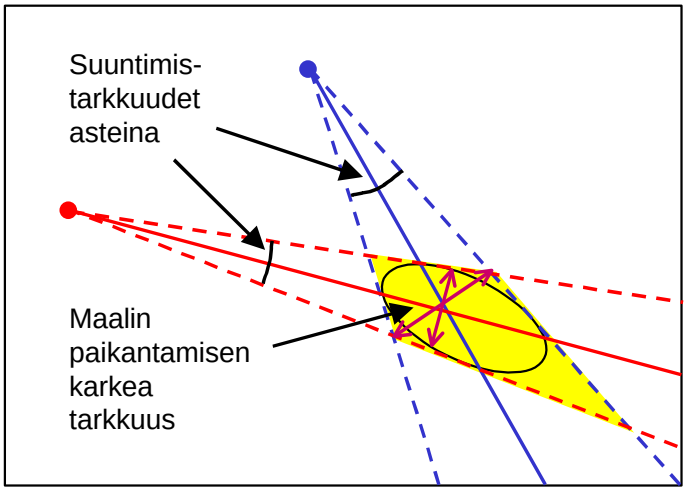
Koska yhdellä suuntimolla ei yleensä pystytä määrittämään maalin etäisyyttä, maalin paikkaa ei voida määritellä. Kahdella tai useammalla suuntimolla kyetään tekemään ristisuuntima, jonka avulla voidaan määrittää lähettimen paikka.




**Kuva L2.2: Paikantamisen poikittainen tarkkuus eri etäisyyksillä suuntimosta. Suuntimistarkkuus voidaan piirtää karttapohjalle suuntiman ympärille kulmamitan avulla (kuvassa katkoviivoilla). Tämä kertoo myös maalin paikantamisen poikittaisen tarkkuuden. Vaihtoehtoisesti, jos maalin etäisyys tunnetaan, poikittainen paikantamistarkkuus metreinä voidaan arvioida karkeasti taulukosta L2.5 ja piirtää janana karttapohjalle kohtisuoraan suuntimaa vastaan.**

Kuvassa L2.2 esitetään yksinkertaisilla välineillä nopeasti tehtävä karkea analyysi maalin paikasta ja sen tarkkuudesta. Kahdella suuntimolla maalin sijainti arvioidaan nelikulmiona, jonka suuntimat ja suuntimistarkkuudet rajaavat. Paikantamisen tarkkuus ilmaistaan käytännössä usein karttapohjalle piirretyllä ellipsillä.

Tutkimalla erilaisia suuntimisgeometrioita voidaan helposti havaita, että paras paikantamisen tarkkuus saavutetaan sijoittamalla suuntimot mahdollisimman lähelle tiedusteltavia kohteita sekä siten, että kohteesta saadut suuntimat ovat mahdollisimman suorassa kulmassa.




**Kuva L2.3: Lähettimen paikka saadaan piirtämällä suuntimat eri sensoreista. Kahden sensorin tapauksessa lähetin on todennäköisimmin suuntimien risteyskohdassa. Kolmen suuntimon tapauksessa lähetin on todennäköisimmin suuntimien rajaaman alueen keskipisteessä. Paikantamistarkkuus saadaan arvioitua karkeasti piirtämällä suuntimistarkkuudet suuntimien ympärille joko kulmamittaa käyttäen tai arvioimalla taulukosta L2.5 kummankin suuntimon poikittainen paikantamistarkkuus metreinä leikkauksen etäisyydellä suuntimosta ja piirtämällä tämä kartalle (violetit janat). Keltainen nelikulmio kuvaa aluetta, jolla maalin voidaan olettaa olevan. Alue ilmaistaan usein nelikulmion sisään piirretyllä ellipsillä.**

## Esimerkki L2.3

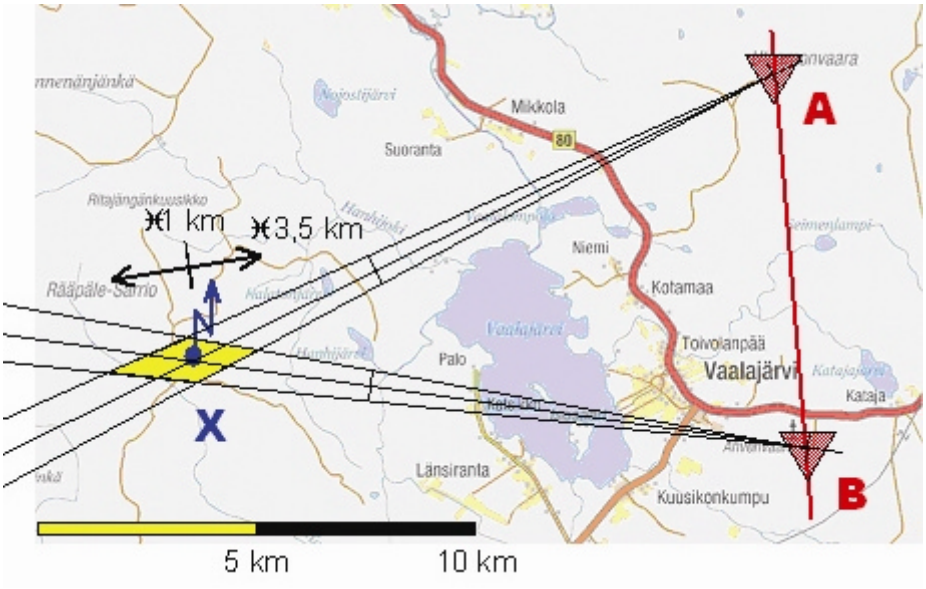
Tarkastellaan kuvassa L2.4 esitettyä tilannetta, jossa halutaan arvioida millä tarkkuudella vastustajan elektroninen tuki kykenee paikantamaan radio-asemamme, joka toimii pisteessä X. Oletetaan, että vastustaja on sijoittanut sensorinsa korkeisiin maastonkohtiin kukkuloille A ja B, joille johtaa ajoneuvo-ura. Vastustajan sensoreiden mittauskannaksi muodostuu tällöin jana AB.

Piirretään pisteistä A ja B suuntimat lähettimen sijaintipaikkaan X.

Oletetaan, että vastustajan suuntimoiden mittaustarkkuus kaikki virhelähteet mukaan lukien on 5 astetta. Sensoreiden tekninen suuntimistarkkuus vaihtelee puolen asteen ja muutaman asteen välillä. Kun lisäksi otetaan huomioon erilaiset muut virhelähteet, voidaan 2-5 asteen suuntimistarkkuutta pitää hyvänä arviona tehtäessä taktisia arvioita.

Seuraavaksi piirretään 5 asteen sektorit kumpaankin suuntimaan. Tällöin syntyy kuvassa keltaisella esitetty nelikulmio, joka kuvaa karkeasti paikantamistarkkuutta.

Kartasta arvioidaan, että vastustaja kykenee paikantamaan lähettimemme noin 1 km x 3,5 km tarkkuudella.




**Kuva L2.4: Vastustajan suuntimoiden arvioidaan toimivan kahden vaaran laella ja havaitsevan noin 15 kilometrin päässä toimivan radioasemamme. Vastustajan suuntimistarkkuudeksi saadaan karkean karttamäärityksen perusteella 1 km x 3,5 km.**

Todetaan, että vastustaja ei kykene määrittämään radion paikkaa tulenkäytön edellyttämällä tarkkuudella, joten se joutuu käyttämään hakeutuvia ammuksia tai suuntaamaan alueelle tiedustelua tai maalinosoituskykyistä tulenjohtovoimaa, mikäli se haluaa lamauttaa radioasemamme.

Edellä esitetty esimerkki antaa karkean kuvan vastustajan paikantamistarkkuudesta. Malli on pelkistetty, joten sitä tulee käyttää vain suuntaa-antavana ja johtopäätösten tekemiseen siitä, miltä alueelta vastustaja kykenee ja miltä se ei kykene paikantamaan lähettimiä suoraan tulenkäytön maaleiksi ja miltä alueilta sen on saatava tarkempi maalinosoitus muilla keinoin.

# LIITE 3: SUOJAUTUMINEN ELEKTRONISELTA HÄIRINNÄLTÄ

Tämä liite pyrkii antamaan vastaukset kysymyksiin:

- Millaisin edellytyksin vastustajan elektroninen häirintä estää järjestelmän toiminnan?
- Minkälaisin keinoin voidaan vähentää vastustajan elektronisen häirinnän vaikuttavuutta?
- Miten tutka- ja viestijärjestelmien suojaaminen voidaan toteuttaa ja miten se vähentää häirinnän vaikutusta?

Asiat kuvataan liitteessä kuvataan riittävästi yleistettyinä ja suhteellisen karkeiden peukalosääntöjen avulla. Näillä mahdollistetaan nopeiden arvioiden tekeminen ilman vaativia laskutoimituksia. Lukijan toivotaan kuitenkin ymmärtävän, että näin saatavat arviot ovat luonteeltaan keskimääräisiä ja yleisiä.

Mikäli tekniikan peruskäsitteet eivät ole lukijalle selviä, häntä kehotetaan lukemaan ensin liite 5.

## Edellytykset järjestelmän häiriintymiselle

Järjestelmän häiriintyminen riippuu siitä, mikä on hyötysignaalin suhde yhteen summautuneeseen häirintäsignaaliin, taustakohinaan ja erilaisiin häiriösignaaleihin (katso kuva 3 johdantoluvussa). Käytännön häirintätilanteissa taustakohina ja häiriöt voidaan yleensä jättää huomioimatta, sillä häirintäsignaali on niitä huomattavasti suurempi. Siten ongelman tarkastelu kulminoituu hyöty- ja häirintäsignaalien suhteeseen (Signal-to-jamming ratio, SJR)[bb]. Pienin järjestelmän normaalin toiminnan mahdollistava SJR riippuu hyvin paljon järjestelmästä itsestään, seuraavassa muutama tätä havainnollistava esimerkki:

- GPS-satelliittipaikannusjärjestelmä (C-koodilla) -40 dB luokkaa
- FSK-kenttäradio 4..6 dB
- GSM-järjestelmäs olosuhteista ja signaalikoodekeista riippuen 4..12 dB
- viranomaisverkon TETRA-radio 15..17 dB

[bb] Itse asiassa kyse on tarkkaan ottaen hyötysignaalin *energian* suhteesta häirintäsignaalin *energiaan*, ei näiden tehojen suhteesta, vaikka tarkastelu käytännössä tehdään useimmiten vertaamalla tehotasoja, kuten tässäkin liitteessä. Asiasta lisätietoja kaipaavaa lukijaa kehotetaan tutustumaan MpKK:n julkaisuun *Digitaalinen taistelukenttä*.

GPS-järjestelmä kykenee siis toimimaan vielä olosuhteissa, joissa häirintäsignaali on 10 000 –kertaa suurempitehoinen kuin vastaanotettu satelliitin lähete! Toista ääripäätä tässä luettelossa edustaa TETRA, jonka radio sietää häiriintymättä häirintäsignaalin, joka on enintään 50-osa hyötysignaalista. Edellä kuvatut esimerkit havainnollistavat, ettei edes karkeiden yleiskäyttöisten peukalosääntöjen antaminen ole mahdollista, vaan häiriintyvyyttä on aina tarkasteltava järjestelmäkohtaisesti. Sotilaskäyttöön suunnitellut viestijärjestelmät tarvitsevat toimiakseen tyypillisesti 3..12 dB hyöty/häirintäsignaalisuhteen. Elektronisesti suojatuissa järjestelmissä (ns. EPM- tai ECCM-laitteet[cc]) erilaiset häirinnänväistömenetelmät voivat laskea häirintäsignaalin tehoa 20..40 dB tai jopa sen ylikin.

Tarkasteltavan järjestelmän ominaisuuksien lisäksi pienin SJR – tai häirintäjärjestelmän kannalta tarkasteltuna vaadittava JSR (Jamming-to-Signal Ratio) – riippuu myös häirintäsignaalin ominaisuuksista, kuten keskitaajuudesta ja kaistanleveydestä sekä muista spektriominaisuuksista, häirintäpulssin pituudesta, pulssintoistotaajuudesta ja käytetystä modulaatiosta tai avainnuksesta. Näitä ei kuitenkaan käsitellä tässä yhteydessä, vaan tarkastelu rajataan SJR/JSR-suhteeseen. Seuraavassa esitetään yleispäteviä keinoja häirinnältä suojautumiseksi.

## Yleisiä toiminnallisia keinoja suojautua häirinnältä

Vastustajan häirinnältä voidaan suojautua teknisin ja toiminnallisin keinoin. Teknisiä keinoja ei käsitellä tässä kirjassa, mutta jälkimmäisiä ovat esimerkiksi:

1. Käytetään suuren vahvistuksen antenneja ja tarvittaessa lisätään lähetystehoa. Suuren lähetystehon käyttämisen ongelmana on kuitenkin se, että se lisää paljastumista vastustajan elektroniselle tuelle. Lähetystehon lisääminen häirinnän seurauksena paljastaa myös häirinnän tehoamisen vastustajan elektronisen tiedustelun tukemalle häirintäyksikölle, joten lähetystehon lisäämistä on tarkasteltava tapauskohtaisesti. Viime kädessä häirinnän ja hyötysignaalin taistelu on kuitenkin taistelua suurimmasta tehosta vastaanottimessa, joten lähetystehon lisääminen on yksi keskeisimpiä häirinnänväistötoimia.
2. Antennin suuri vahvistus liittyy myös antennin suuntaavuuteen: mitä suurempi vahvistus antennilla on, sitä suuremman osan lähetettävästä tehosta se säteilee pääkeilan suuntaan ja sitä kapeampi pääkeila on. Vastaavasti muihin suuntiin säteilyteho on pienempi. Tämän vuoksi voimakkaasti suuntaavia antenneja käytettäessä vastustaja ei saa helposti häirintäsignaaliaan omaan pääkeilaamme, vaan joutuu toimimaan heikomman vahvistuksen sivukeiloista. Antennivahvistuksen lisääminen ei aina ole mahdollista, esimerkiksi valvontatutka tai uhkavaroitukseen käytettävä elektronisen tuen sensori ei voi olla kovin kapeakeilainen valvottavan alueen laajuuden vuoksi.

[cc] EPM =Electronic Protective Measures, eli elektroniset suojautumiskeinot. ECCM = Electronic Counter Counter-Measures, eli vastatoimet elektronisille vastatoimille (=häirinnälle).

3. Suunnitellaan viestiverkko siten, ettei suuntaavien antennien pää- ja takakeiloja tai suurimpia sivukeiloja kohdistu pahimpiin uhkasuuntiin. Esimerkiksi linkkiverkko tulisi suunnitella vinosti häirintälähetinten todennäköisimpiä suuntia kohtaan. Tällöin linkkien pääkeilat eivät suuntaudu häirintälähettimiin päin.

4. Pyritään minimoimaan häirinnän vaikutus kääntämällä suuntaavan antennin säteilyminimi häirintäjärjestelmän suuntaan. Vaikka tällöin voidaan joutua suuntaamaan pääkeila pois vastaanottimesta, on ratkaisu yleensä oikea, sillä aina kun sivukeilanvahvistus häirintäjärjestelmän suuntaan heikkenee enemmän kuin pääkeilan vahvistus vastaanottimen suuntaan, vastaanotetun signaalin suhde häirintäsignaaliin kasvaa ja tilanne paranee.

5. Suunnitellaan viesti- tai tutkaverkko siten, että viestiverkossa yhteysväli ja tutkaverkossa maalin etäisyys on uhkaan (häirintälähettimen etäisyyteen) nähden riittävän pieni.

6. Sijoitetaan viestiasemat siten, että etenemisvaimennus häirintälähettimen suuntaan on mahdollisimman suuri hyödyntämällä maastoesteitä ja korkeilla taajuuksilla myös rakennuksia ja kasvillisuutta.

7. Vaikeutetaan vastustajan signaalitiedustelua ja elektronista tukea millä keinolla hyvänsä, sillä häirintä tarvitsee lähes aina tuekseen häirittävää kohdetta havainnoivaa vastaanotintekniikkaa. Tällaista vaikeuttamista voi olla esimerkiksi omat lähetteet peittävä (maskaava) vastustajan suuntaan lähetetty häirintä tai signaalin kätkentä spektrin ruuhkaisemmille alueille muiden lähetteiden sekaan.

8. Estetään vastustajan signaalitiedustelua ja elektronista tukea tunnistamasta järjestelmäämme, edes toiminnan kriittisemmän hetken ajaksi. Näin voidaan pyrkiä tekemään esim. salaamalla osa järjestelmiemme parametriavaruudesta (ns. sotamoodit) ja hankkimalla useita samoilla taajuusalueilla ja muilla samantyyppisillä parametreilla toimivia järjestelmiä sekä harhautus-lähettimiä.

9. Toimitaan mahdollisimman laajakaistaisesti ja/tai nopealla taajuushyppelyllä, mikä voi pakottaa vastustajan häirinnän laajakaistaiseksi ja pienentämään yhdelle taajuudelle lähettämäänsä häirintätehoa. Mikäli vastustajan häirintälähetin ei pysty seuraamaan taajuushypytystä tai häiritsemään laajakaistaisesti yhtä laajalla kaistalla, häirintä ei välttämättä ole tehokasta.

10. Sammutetaan tutkajärjestelmän lähetin häirintälähettimen suuntaan toimittaessa, mikäli kyseessä ei ole tärkeän maalin suorittama omasuoja-häirintä. Omasuojahäirinnän tapauksessa häirintä voidaan suuntia – mikäli useampia tutkia tai elektronisen tuen järjestelmiä on verkotettu, voidaan niillä ristisuuntia ja siten paikantaa maali.

11. Tehdään sensoriverkosta tarpeeksi tiheä, jotta omasuojahäirintää käyttävät lavetit joutuvat toimimaan tutkan läpipolttoetäisyydellä.

12. Luodaan harhautusviestiverkkoja ja mahdollisesti harhautussensoreita, joiden häirintään sitoutuu vastustajan resursseja.

13. Tuhotaan fyysisesti vastustajan häirintälähettimet.
14. Estetään erikoisjoukkoja asettamasta lähihäirintälähettimiä.
15. Luodaan valmius paikantaa vastustajan lähihäirintälähettimet tai valmistaudutaan siirtymään nopeasti pois niiden läheisyydestä.

Häirinnän tehoamista ei tule paljastaa vastustajalle. Vastustajan häirintäjärjestelmä voi perustaa häirintätaktiikkansa viestijärjestelmästä tai tutkista sieppaamiensa signaalien analysointiin[dd]. Mikäli häiritty viestijärjestelmä lisää lähetystehoa tai etsii häirinnästä vapaata kanavaa tai tutkajärjestelmä siirtyy eri moodiin, häirintäjärjestelmä tietää häirinnän tehonneen. Jos järjestelmän käyttöä jatketaan samaan tapaan kuin ennen häirinnän tehoamista, häirintälähetin joko jatkaa häirintää tietämättä sen tehoamista tai lakkaa häiritsemästä sitä ja siirtyy toiselle taajuudelle[ee]. Edellisessä tapauksessa osa häirintälähettimen tehosta sitoutuu tämän yhteyden häirintään ja on poissa jonkin muun järjestelmän häirinnästä, jälkimmäisessä tapauksessa tuloksena on häirinnän päättyminen.

Käytännön tilanne ei luonnollisesti ole näin yksinkertainen – järjestelmien häirinnänväistöominaisuudet on suunniteltu käyttöä varten, joten taktisessa tilanteessa tulee kyetä punnitsemaan häirinnän tehoamisen paljastumisen ja häirinnän väistön tuovan hyödyn välinen ristiriita. Lisäongelman tuo myös häirinnänväistömenetelmien paljastuminen vastustajan tiedustelulle, mikäli kyseisiä moodeja käytetään liian herkästi. Tällaiset ratkaisut tulisi ohjeistaa keskitetysti esim. voimankäytön säännöksissä, eikä jättää yksittäisen operaattorin ratkaistaviksi.

Häirinnältä suojautumista voidaan arvioida samoin kuin elektroniselta tiedustelulta ja valvonnalta suojautumista liitteessä 2. Pääosin samojen vaimenemis- ja tehokaavojen avulla voidaan laskea signaalivoimakkuuksia ja vaimenemisia, ja arvioida saako hyöty- vai häirintäsignaali voiton oman järjestelmämme vastaanottimessa.

Häirintään liittyviä teknisiä käsitteitä käsitellään lyhyesti myös aiemmissa tekstiluvuissa.

---

[dd] Lisäksi pitkän tähtäimen häirintämenetelmä- tai häirintäjärjestelmäkehitys voi perustua niihin tietoihin järjestelmien häirinnänväistö- ja muista ominaisuuksista, jotka on säteilty taivaalle ”vahingossa” vuosien varrella.

[ee] R. V. Jones kertoo kirjassaan *Most Secret War*, kuinka britit saivat saksalaiset lopettamaan Maltalla sijaitsevien ilmavalvontatutkien häirinnän, vaikka häirintä tehosi niin hyvin, ettei brittien ilmapuolustus kyennyt hyödyntämään tutkia lainkaan. Keino oli yksinkertainen: kun häirintä oli aiemmin estänyt tutkien käytön, britit olivat sammuttaneet ne tarpeettomina. Saksalaisten signaalitiedustelu tiesi siis häirinnän tehonneen, kun se ei kyennyt enää havaitsemaan tutkasignaalin pyyhkäisyä. Kun britit oivalsivat tämän, he jatkoivat tutkaamista, vaikkei tutkalla mitään nähnytkään. Tämän seurauksena Luftwaffe päätteli jonkinlaisen uuden häirinnänväistömenetelmän tulleen käyttöön eikä häirintä enää tehoaisi. Niinpä se lopetettiin eivätkä saksalaiset enää yrittäneet häiritä brittien ilmapuolustusta.

## Viestijärjestelmien suojaaminen

Viestijärjestelmien häirinnältä suojautumisen arviointi tapahtuu pitkälti samoin menetelmin kuin liitteessä 2 kuvattiin. Liitteessä 2 arvioitiin oman hyötylähetteen etenemistä vastustajan tiedustelujärjestelmään eli yhtä radioyhteysväliä. Häirintää arvioitaessa on tarkasteltava kahta eri radioyhteyttä: omasta lähettimestä yhteysvälin toiseen päähän omaan vastaanottimeen, ja vastustajan häirintälähettimestä omaan vastaanottimeen.

Yhteysvälit eivät ole identtisiä pituutensa suhteen, mutta eivät yleensä myöskään oman vastaanottoantennimme antennivahvistuksen suhteen. Viestiyhteytemme häiritsijä on usein antennimme heikommassa sivukeilassa, sillä antennin pääkeila on yleensä suunnattu vasta-asemaan päin. Erityisen ikävä on tilanne, jossa häiritsijä on pääkeilan suunnassa; tällainen tilanne voi syntyä esimerkiksi lähihäirintälähettimien tai lennokkiin sijoitetun häirintälähettimen tapauksessa, jos linkkiyhteydet on suunniteltu huonosti osoittamaan kohti pääuhkasuuntaa, kun kyseessä on vastustajan selustassa toimiva partio tai käytännössä yleisimmin ympärisäteilevien antennien tapauksessa (esim. kenttäradio marssiantennilla).

Häirittävyysanalyysissä täytyy myös tietää, millainen häirintä-signaalisuhde, siis omaan vastaanottimeen saapuvan häirintäsignaalin tehon suhde vastaanottimeen saapuvaan hyötysignaalin tehoon, on kriittinen oman vastaanottimen kannalta. Yleensä laskuissa käytetään kriittisenä rajana häirintä-signaalisuhdetta 1 (0 dB). Tällöin häirintäsignaali on yhtä vahva kuin hyötysignaalikin, minkä karkeassa arviossa katsotaan riittävän estämään viestiyhteyden syntymisen.

Vaadittava häirintä-signaalisuhde vaihtelee huomattavasti eri järjestelmissä. Häirintää kestämään tarkoitetuissa hajaspektrijärjestelmissä voidaan vaatia tuhansia – kymmeniä tuhansia kertoja hyötysignaalia suurempi (+20..30 dB) häirintäteho yhteyden katkaisemiseen, kun taas herkimmät järjestelmät eivät välttämättä kestä hyötysignaaliin verrattuna edes kymmenes – sadasosien suuruista (-10..-20 dB) häirintäsignaalia. Esimerkiksi perinteinen AM-puheyhteys, sähkötyksestä puhumattakaan, on melko häiriösietoinen. Sen sijaan esimerkiksi viranomaisverkko ja matkapuhelimet ovat hyvinkin herkkiä häirinnälle.

Pelkkä häirintäteho ei ole riittävä parametri häirinnän onnistumista arvioitaessa. Nykyisissä digitaalilähetteissä on tehokkaita virheenkorjaustoimintoja, joiden avulla häirinnän vaikutusta voidaan vähentää. Toisaalta digitaalijärjestelmissä käytettävät tiedonsiirtokehykset ovat herkkiä jo muutamien bittien virheille. Tämän vuoksi häirinnän ei tarvitse olla jatkuvaa: sopivan voimakkaat lyhytkestoiset satunnaiset pulssit voivat esimerkiksi estää tiedonsiirtolinkin synkronoitumisen kohtuullisen pitkäksikin aikaa, vaikka keskimääräinen häirintäteho olisi pieni. Taajuushyppiville lähetteille puolestaan voidaan määrittää kriittinen osuus hypyistä (esim. 20%), jota suuremman osan häiritseminen estää viestin läpimenon. Tällöin, mikäli häiritsijä ei kykene seuraamaan lähetettä taajuushyppy hypyltä, se voi miettiä häirintätaktiikkaansa: jos käytettävissä on vain tietty määrä lähetystehoa, jakaako

tehoaan laajemmalle kaistalle ja pyrkiä ajallisesti koko lähetteen häirintään, vai keskittyäkö kapeampaan taajuuskaistaan, saavuttaa suurempi tehotiheys näillä taajuuksilla, ja pyrkiä häiritsemään vähintäänkin kriittinen osuus ajanhetkistä.

Häirinnältä suojautumisen analysointi vaatii siis paljon tietoa omasta viesti-järjestelmästä. Karkean arvion voi kuitenkin laskea häirintä-signaalisuhteella 1. Ensimmäiseksi lasketaan hyötysignaalin teho vastaanottimessa, mikä tapahtuu liitteen 2 kaavoja soveltamalla *desibeleinä* seuraavasti:

$$S = P_{LS} + G_{LS} - L_S + G_{VS}$$

missä $S$ on oman hyötysignaalimme teho vastaanottimessa, $P_{LS}$ oman lähettimemme lähetysteho, $G_{LS}$ lähettimemme antennivahvistus oman vastaan-ottimemme suuntaan (pääkeilavahvistus), $L_S$ lähetteemme yhteysvälivaimennus ja $G_{VS}$ vastaanottimemme antennivahvistus oman lähettimemme suuntaan (pääkeila-vahvistus)[ff]. Yhteysvälivaimennus lasketaan kuten liitteessä 2 esitettiin, esimerkiksi taulukoita L2.2 tai L2.4 soveltaen.

Vastaavasti lasketaan häirintäsignaalin teho omassa vastaanottimessamme *desibeleinä:*

$$J = P_{LJ} + G_{LJ} - L_J + G_{VJ}$$

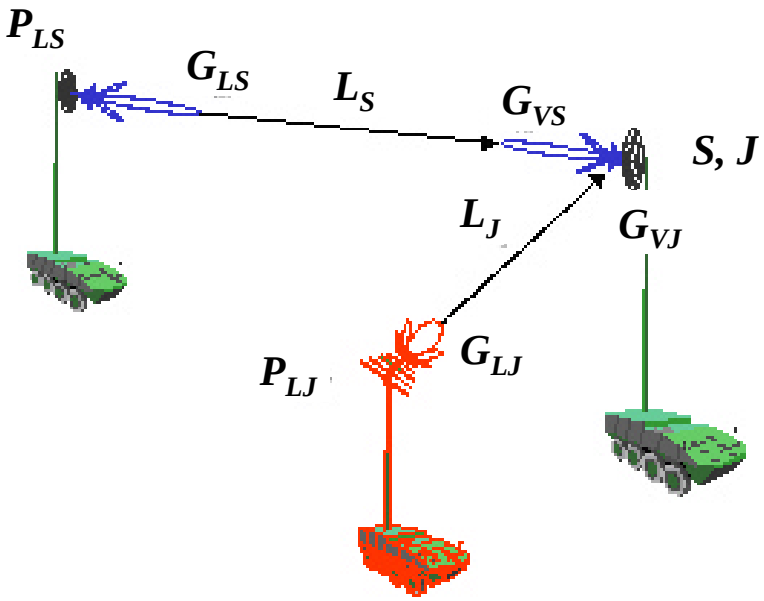
missä $J$ on häirintäsignaalin teho omassa vastaanottimessamme, $P_{LJ}$ häirintälähettimen lähetysteho, $G_{LJ}$ häirintälähettimen antennivahvistus oman vastaan-ottimemme suuntaan, $L_J$ häirintälähetteen yhteysvälivaimennus ja $G_{VJ}$ vastaan-ottimemme antennivahvistus häirintälähettimen suuntaan (usein sivukeilavahvistus). Yhteysvälivaimennus lasketaan kuten edellä, mutta on huomattava, että hyöty- ja häirintäsignaaleilla voi olla täysin erilaiset vaimennustilanteet, jos esim. hyöty-lähetteemme etenee peitteisessä maastossa ja häirintälähetin on korkealla ilmassa vapaassa tilassa.

Vertaamalla saatuja tehoja $S$ ja $J$ voidaan arvioida häirinnän onnistumista: karkean arvion mukaan häirintä on siis tehokasta, jos $J > S$.

**Esimerkki L3.1**

Arvioidaan pitkälanka-antenneilla sekä lähetys- että vastaanottopäässä varustetun 50 MHz:n kenttäradioyhteyden häirittävyyttä. Oletetaan, että kenttäradion lähetysteho on 10 W (=40 dBm), yhteysväli 10 km ja oma yhteys on kummankin pitkälanka-antennin pääkeilassa, joiden vahvistus on 8 dB.

[ff] Alaindeksien määrää täytyi kasvattaa liitteestä 2, koska nyt täytyy laskea kahden eri radioyhteyden tekijöitä. Alaindekseissä kirjaimet valittiin viittaamaan lähetykseen/vastaanottoon (L/V) ja hyötysignaaliin/häirintään (S/J).




**Kuva L3.1: Kaavoissa ja esimerkkilaskuissa käytettävien parametrien lyhenteet.**

Kenttäradioyhteys ei ole vapaassa tilassa, jolloin karkea arvio yhteysväli-vaimennuksesta saadaan liitteen 2 mukaisesti esim. Eglin mallista. Mikäli molemmat antennit olisivat 1 m korkeudella, olisi yhteysvälivaimennus taulukon L2.4 mukaan hyvin karkeasti noin 150 dB[gg]. Tällöin hyötysignaalin teho vastaanottimessa on em. kaavan mukaisesti $S$ = 40 dBm + 8 dB - 150 dB + 8 dB = -94 dBm.

Tarkastellaan tilannetta, jossa vastustaja käyttää erikoisjoukkojensa asentamaa lähihäirintälähetintä, jolla on 1 W:n (=30 dBm) lähetysteho ja ympärisäteilevä marssiantenni ($G_{LJ}$ = 0 dB), siten että lähetin on 1 km:n päässä omasta vastaanottoantennistamme, sen sivukeilassa. Laskua varten täytyy tietää oman vastaanottoantennimme vahvistus (tai sivukeilataso) häirintälähettimen suuntaan. Oletetaan, että pitkälanka-antennin vahvistus häirintälähettimen suuntaan on $G_{VJ}$ = 0 dB, ja yhteysvälivaimennus arvioidaan Eglin mallin mukaisesti (1 m:n antennikorkeuksilla taulukon L2.4 mukaan $L_J$ = 110 dB). Tällöin häirintäsignaalin tehoksi omassa vastaanottimessamme saadaan $J$ = 30 dBm + 0 dB – 110 dB + 0 dB = -80 dBm.

Häirintäteho vastaanottimessa on siis 14 dB voimakkaampaa kuin hyöty-signaalimme teho, ja häirintä on tämän karkean arvion mukaan tehokasta. Mikäli häirintä tapahtuisi lennokista vapaassa tilassa muuten samalla häirintäjärjestelmällä ja tilanteessa, saataisiin taulukon L2.2 vapaan tilan vaimennusta hyödyntäen vielä 200 km:n etäisyydellä vastaanottimesta saman suuruusluokan häirintäteho $J$ = 30 dBm + 0 dB - 112 dB + 0 dB = -82 dBm.

[gg] Pitkälanka-antennia ei toki kannata virittää 1 m korkeuteen, mutta yksinkertainen arvio löytyi taulukosta. Liitteen 2 Eglin kaavasta voidaan laskea, että 2 m korkeudella olevilla antenneilla yhteysvälivaimennus olisi 141 dB, 3 m korkeudella 136 dB jne.

| | 1 km | 2 km | 5 km | 10 km | 20 km | 50 km | 80 km |
|---|---|---|---|---|---|---|---|
| **Kenttäradiot (*f*=50 MHz, kiinteä- ja hyppivätaajuinen)** | | | | | | | |
| - *P*=1 W, *G*=0 dB (marssiantenni 1m) | -80 | -92 | -108 | -120 | -132 | -148 | -156 |
| - *P*=5 W, *G*=0 dB (marssiantenni 1m) | -73 | -85 | -101 | -113 | -125 | -141 | -149 |
| - *P*=50 W, *G*=0 dB (ajoneuvoant. 3m) | -49 | -61 | -77 | -89 | -101 | -117 | -125 |
| - *P*=1 W, *G*=8 dB (pitkäl.ant. 2m) | -55 | -67 | -83 | -95 | -107 | -123 | -131 |
| - *P*=5 W, *G*=8 dB (pitkäl.ant. 2m) | -48 | -60 | -76 | -88 | -100 | -116 | -124 |
| - *P*=50 W, *G*=8 dB (ajoneuvoant. 3m) | -33 | -45 | -61 | -73 | -85 | -101 | -109 |
| **Lentokoneradio (*f*=300 MHz)** | | | | | | | |
| - *P*=5 W, *G*=2 dB | -41 | -47 | -55 | -61 | -67 | -75 | -79 |
| - *P*=10 W, *G*=2 dB | -38 | -44 | -52 | -58 | -64 | -72 | -76 |
| - *P*=20 W, *G*=2 dB | -35 | -41 | -49 | -55 | -61 | -69 | -73 |
| **Kenttälinkki (*f*=800 MHz)** | | | | | | | |
| - *P*=1 W, *G*=15 dB (antenni 10m) | -44 | -56 | -72 | -84 | -96 | -112 | -120 |
| - *P*=10 W, *G*=15 dB (antenni 10m) | -34 | -46 | -62 | -74 | -86 | -102 | -110 |
| **Mikroaaltolinkki (*f*=8 GHz)** | | | | | | | |
| - *P*=0,1 W, *G*=35 dB | -21 | -27 | -35 | -41 | -47 | -55 | -59 |
| - *P*=1 W, *G*=35 dB | -11 | -17 | -25 | -31 | -37 | -45 | -49 |

**Taulukko L3.1: Viestijärjestelmien hyötysignaalitehoja dBm-yksiköissä vastaanottimessa erilaisilla toimintaparametreilla ja yhteysetäisyyksillä[hh,ii]. Vertaa näitä arvoja taulukon L3.2 häirintätehoihin samoissa vastaanottimissa.**

Tämä havainnollistaa kahden tärkeän seikan merkitystä: häirintä on erityisen tehokasta, kun se suoritetaan

1. Läheltä: lähellä oleva pienitehoinenkin häirintälähetin voi estää viestiyhteydet.
2. Ilmasta: vapaan tilan vaimennus on niin pieni verrattuna muihin vaimennuksiin, että pienitehoinen lähetin on tehokas hyvinkin kaukaa, mikäli se saadaan maastoesteiden yläpuolelle.

[hh] Yhteysvälivaimennukset on laskettu vapaan tilan vaimennuksen tai Eglin vaimennusmallin mukaan tilanteesta riippuen. Mikroaaltolinkki on kuitenkin ongelma, koska sen taajuus (8 GHz) ei ole Eglin mallin pätevyysalueella (30-1000 MHz). Tässä esimerkissä käytettäväksi valittiin vapaan tilan vaimennus, koska yhteyden voidaan tässä tapauksessa olettaa olevan vapaassa tilassa.

[ii] Eglin vaimenemismallilla laskettavien järjestelmien yhteydessä on ilmoitettu käytetty antennikorkeus, joka vaikuttaa yhteysvälivaimennukseen.

| | 1 km | 2 km | 5 km | 10 km | 20 km | 50 km | 80 km |
|---|---|---|---|---|---|---|---|
| **Häirintälentokone (*P*=1 kW, *G*=3 dB)** | | | | | | | |
| - Kiinteätaajuinen kenttäradio, marssiant. | -3 | -9 | -17 | -23 | -29 | -37 | -42 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 100 kanavaa | -23 | -29 | -37 | -43 | -49 | -57 | -62 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 5000 kanavaa | -40 | -46 | -54 | -60 | -66 | -74 | -78 |
| - Kiinteätaajuinen kenttäradio, suunta-ant. | 5 | -1 | -9 | -15 | -21 | -29 | -34 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 100 kanavaa | -15 | -21 | -29 | -35 | -41 | -49 | -54 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 5000 kanavaa | -32 | -38 | -46 | -52 | -58 | -66 | -70 |
| - Lentokoneradio | -17 | -23 | -31 | -37 | -43 | -51 | -55 |
| - Kenttälinkki | -13 | -19 | -27 | -33 | -39 | -47 | -51 |
| - Mikroaaltolinkki | -13 | -19 | -27 | -33 | -39 | -47 | -51 |
| **Takt. häirintälavetti (*P*=100 W, *G*=6 dB)** | | | | | | | |
| - Kiinteätaajuinen kenttäradio, marssiant. | -34 | -46 | -62 | -74 | -86 | -102 | -110 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 100 kanavaa | -54 | -66 | -82 | -94 | -106 | -122 | -130 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 5000 kanavaa | -71 | -83 | -99 | -111 | -123 | -139 | -147 |
| - Kiinteätaajuinen kenttäradio, suunta-ant. | -22 | -34 | -49 | -62 | -74 | -89 | -98 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 100 kanavaa | -42 | -54 | -69 | -82 | -94 | -109 | -118 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 5000 kanavaa | -58 | -71 | -86 | -98 | -111 | -126 | -135 |
| - Lentokoneradio | -24 | -30 | -38 | -44 | -50 | -58 | -62 |
| - Kenttälinkki | -33 | -45 | -61 | -73 | -85 | -101 | -109 |
| - Mikroaaltolinkki | -20 | -26 | -34 | -40 | -46 | -54 | -58 |
| **Lähihäirintälähetin (*P*=1 W, *G*=2 dB)** | | | | | | | |
| - Kiinteätaajuinen kenttäradio, marssiant. | -78 | -90 | -106 | -118 | -130 | -146 | -154 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 100 kanavaa | -98 | -110 | -126 | -138 | -150 | -166 | -174 |
| - Hyppivätaajuinen kenttäradio, marssiantenni, 5000 kanavaa | -115 | -127 | -143 | -155 | -167 | -183 | -191 |
| - Kiinteätaajuinen kenttäradio, suunta-ant. | -66 | -78 | -93 | -106 | -118 | -133 | -142 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 100 kanavaa | -86 | -98 | -113 | -126 | -138 | -153 | -162 |
| - Hyppivätaajuinen kenttäradio, suunta-antenni, 5000 kanavaa | -102 | -115 | -130 | -142 | -155 | -170 | -179 |
| - Lentokoneradio | -48 | -54 | -62 | -68 | -74 | -82 | -86 |
| - Kenttälinkki | -77 | -89 | -105 | -117 | -129 | -145 | -153 |
| - Mikroaaltolinkki | -44 | -50 | -58 | -64 | -70 | -78 | -82 |

**Taulukko L3.2. Häirintäjärjestelmien aiheuttamia häirintätehoja taulukon L3.1 järjestelmien vastaanottimiin niiden pääkeilassa. Eglin vaimennus on laskettu taulukon L3.1 antennikorkeuksille, häirintäantennin korkeudelle 10 m ja lähihäirintälähettimen antennikorkeudelle 1 m.**

Taulukoissa L3.1 ja L3.2 on lisää mahdollisia esimerkkejä hyöty- ja häirintäsignaaleiden tehoista vastaanottimessa, joiden avulla häirinnän tehokkuutta voi arvioida erilaisilla viesti- ja häirintäetäisyyksillä[jj]. On muistettava, että usein häirintä tapahtuu sivukeilasta, jolloin häirintätehosta tulee vähentää sivukeilataso (esim. linkkien tapauksessa tyypillisesti 15-35 dB tai enemmän) kyseiseen suuntaan. Taulukosta havaitaan myös nopean taajuushypytyksen vaikutus häirintätehoon. On toki huomattava, ettei yksi häirintälähetinyksilö käytännössä kykene kaikkien listattujen viestijärjestelmien häirintään, kyse on vain tehotarkastelusta. Taulukossa L3.2 oletetaan, hyppivätaajuisten radioiden häirinnän yhteydessä, ettei häirintäjärjestelmä kykene seuraamaan taajuutta hyppy hypyltä, vaan joutuu jakamaan häirintätehonsa laajemmalle kaistalle, mainitulle kanavamäärälle. Mikäli häirintälähetin kykenee seuraamaan lähetystaajuutta ja toimimaan tehokkaasti aina kapealla taajuuskaistalla kerrallaan, häirintätilanne vastaa perinteistä yksitaajuista analogista kenttäradiota.

**Esimerkki L3.2**

Tarkastellaan kenttälinkin (800 MHz, 1 W, 15 dB) häirittävyyttä ***ilmasta*** tilanteessa, jossa kahden radion väli on 20 km ja häiritsijä toimii 50 km etäisyydeltä. Arviointi suoritetaan taulukoiden avulla seuraavasti:

1. Katsotaan taulukosta L3.1 hyötysignaalin teho vastaanottimessa. Mikäli lähetysteho on 1 W, on hyötysignaaliteho taulukon mukaan -96 dBm.

2. Katsotaan taulukosta L3.2 häirintäsignaaliteho vastaanottimessa kyseisessä häirintälentokoneen ja kenttälinkin tilanteessa. Taulukon mukaan häirintäteho vastaanottimessa on pääkeilasta häirittäessä -47 dBm.

3. Häirintäsignaali on siis 49 dB voimakkaampaa kuin hyötysignaali. Häirintä on hyvin tehokasta.

Tarkastellaan erilaisia variaatioita: Kenttälinkin lähetystehon nostaminen 10 wattiin parantaisi tilannetta linkin kannalta 10 dB, häiritsijän toiminta sivukeilassa pääkeilan ja sivukeilan vahvistusten erotusten verran. Kiinteällä kapeakaistaisella taajuudella toimittaessa (ei hajaspektri-ominaisuuksia) tilanne on kuitenkin melko epätoivoinen kenttälinkin kannalta, häiritsijän päästessä näinkin lähelle.

Esimerkki voidaan myös laskea kaavoilla, jos taulukoita ei haluta tai voida käyttää. Tällöin toimitaan seuraavasti:

1. Lasketaan hyötysignaaliteho vastaanottimessa kaavalla

   $S = P_{LS} + G_{LS} - L_S + G_{VS}$:

[jj] Häirintälentokoneeseen, lentokoneradioon ja 8 GHz:n linkkiin liittyvät yhteydet on laskettu vapaan tilan vaimennuksella, muut Eglin mallilla.

- Lähetysteho on esimerkissä $P_{LS}$ = 1 W = 10 x $\log_{10}(1)$ = 0 dBW = 0 + 30 dBm = 30 dBm.
- Kenttälinkin lähetysyksikön antennivahvistus vastaanottimen suuntaan on $G_{LS}$ = 15 dB.
- Kenttälinkkiyhteys ei ole vapaassa tilassa (pinnasta-pintaan-yhteys) ja Eglin mallin reunaehdot ovat voimassa, joten lasketaan yhteysvälivaimennus Eglin mallin mukaisesti liitteen 2 kaavalla:

$$L_S = L_E = 76{,}3 + 20 \times \log_{10}(800) + 40 \times \log_{10}(20) - 20 \times \log_{10}(10) - 10 \times \log_{10}(10)$$
$$= 156 \text{ dB}$$

- Kenttälinkin vastaanottoyksikön antennivahvistus lähettimen suuntaan on $G_{VS}$ = 15 dB.
- Lasketaan kenttälinkin hyötysignaaliteho sen vastaanottimessa:

$$S = 30 \text{ dBm} + 15 \text{ dB} - 156 \text{ dB} + 15 \text{ dB} = -96 \text{ dBm}.$$

2. Lasketaan häirintäteho vastaanottimessa kaavalla:

$$J = P_{LJ} + G_{LJ} - L_J + G_{VJ}:$$

- Häirintälentokoneen lähetysteho on esimerkissä $P_{LJ}$ = 1 kW = 1000 W = 10 x $\log_{10}(1000)$ = 30 dBW = 30 + 30 dBm = 60 dBm.
- Häirintäjärjestelmän antennivahvistus häirittävän järjestelmän suuntaan on $G_{LJ}$ = 3 dB.
- Häirintäyhteyden voidaan olettaa olevan vapaassa tilassa, koska kyseessä on korkealla toimiva lentokone (tätä voidaan tutkia radiohorisontin kaavalla tai taulukolla). Tällöin vaimennus voidaan laskea vapaan tilan vaimennuksen kaavalla liitteen 2 mukaisesti:

$$L_J = L_V = 32{,}4 + 20 \times \log_{10}(50) + 20 \times \log_{10}(800)$$
$$= 32{,}4 + 34{,}0 + 58{,}1$$
$$= 125 \text{ dB}$$

- Kenttälinkin vastaanottoyksikön antennivahvistus häirintäjärjestelmän suuntaan on (pääkeilahäirinnän tapauksessa) $G_{VJ}$ = 15 dB.
- Lasketaan häirintäteho kenttälinkkijärjestelmän vastaanottimessa $J$ = 60 dBm + 3 dB - 125 dB + 15 dB = -47 dBm.

3. Häirintäsignaali on siis -47 dBm - (-96 dBm) = 49 dB voimakkaampaa kuin hyötysignaali. Pääkeilahäirintä on hyvin tehokasta.

4. Em. kaavojen avulla erilaisia variaatioita tehoihin, etäisyyksiin ja antennivahvistuksiin voidaan tarkastella hyvin vapaasti.

**Esimerkki L3.3**

Tarkastellaan marssiantennilla varustetun kenttäradion (50 MHz, 5 W, 0 dB) häirittävyyttä ***pinnasta*** tilanteessa, jossa kahden radio väli on 5 km ja taktinen häirintälavetti toimii 20 km:n etäisyydeltä. Arviointi suoritetaan taulukoiden avulla seuraavasti:

1. Katsotaan taulukosta L3.1 hyötysignaalin teho vastaanottimessa kyseissä tilanteessa. Mikäli lähetysteho on 5 W ja käytössä on marssiantenni, on hyötysignaaliteho taulukon mukaan -101 dBm.
2. Katsotaan taulukosta L2.2 häirintäsignaaliteho vastaanottimessa kyseisessä tilanteessa. Taktiselle häirintälavetille häirintäsignaaliteho vastaanottimessa on kyseissä tilanteessa -86 dBm.
3. Häirintäsignaali on siis 15 dB voimakkaampaa kuin hyötysignaali. Häirintä on tehokasta.

Tarkastellaan erilaisia variaatioita: Pitkälanka-antennin käyttäminen nostaisi hyötytehoa taulukon mukaan huomattavasti arvoon -76 dBm. Pääkeilahäirintäkin nousisi tällöin arvoon -74 dBm, mutta arvot ovat jo samaa suuruusluokkaa ja viesti saattaisi hyvinkin päästä perille – ainakin ajoittain. Mikäli häiritsijä voitaisiin sulkea vastaanottimen pitkälanka-antennin pääkeilan ulkopuolelle, mikä on usein mahdollista käytännön taktisessa tilanteessa, yhteys saataisiin läpi.

Edellä kuvattu esimerkki voidaan myös laskea kaavoilla, jos taulukoita ei haluta käyttää tai niiden arvot eivät riitä. Tällöin toimitaan seuraavasti:

1. Lasketaan hyötysignaaliteho vastaanottimessa kaavalla

   $S = P_{LS} + G_{LS} - L_S + G_{VS}$:

   - Lähetysteho on esimerkissä $P_{LS}$ = 5 W = 10 x $\log_{10}(5)$ = 7 dBW = 7 + 30 dBm = 37 dBm.
   - Kenttäradion marssiantennin antennivahvistus vastaanottimen suuntaan on $G_{LS}$ = 0 dB.
   - Kenttäradioyhteys ei ole vapaassa tilassa (pinnasta-pintaan-yhteys) ja Eglin mallin reunaehdot ovat voimassa, joten lasketaan yhteysvälivaimennus Eglin mallin mukaisesti liitteen 2 kaavalla:

     $$L_S = L_E = 76{,}3 + 20 \times \log_{10}(50) + 40 \times \log_{10}(5) - 20 \times \log_{10}(1) - 10 \times \log_{10}(1)$$
     $$= 138 \text{ dB}$$

   - Vastaanottavan kenttäradion antennivahvistus lähettimen suuntaan on $G_{VS}$ = 0 dB.

- Lasketaan kenttäradion hyötysignaaliteho vastaanottimessa $S$ = 37 dBm + 0 dB – 138 dB + 0 dB = –101 dBm.

2. Lasketaan häirintäteho vastaanottimessa kaavalla

   $J = P_{LJ} + G_{LJ} - L_J + G_{VJ}$:

   - Häirintäjärjestelmän lähetysteho on esimerkissä $P_{LJ}$ = 100 W = 10 x $\log_{10}$(100) = 20 dBW = 20 + 30 dBm = 50 dBm.
   - Häirintäjärjestelmän antennivahvistus häirittävän kenttäradion suuntaan on $G_{LJ}$ = 6 dB.
   - Koska häirintä tapahtuu pinnasta pintaan, kyseessä ei voi olla vapaan tilan vaimeneminen. Taajuuden ja yhteysvälin puolesta Eglin mallia voidaan käyttää, jolloin vaimennus voidaan laskea liitteen 2 mukaisesti:

     $$L_S = L_E = 76{,}3 + 20 \times \log_{10}(50) + 40 \times \log_{10}(20) - 20 \times \log_{10}(10) - 10 \times \log_{10}(1) = 142 \text{ dB}$$

   - Kenttäradion antennivahvistus (ympärisäteilevä marssi-antenni) häirintäjärjestelmän suuntaan on $G_{VJ}$ = 0 dB.
   - Lasketaan häirintäteho kenttälinkkijärjestelmän vastaan-ottimessa $J$ = 50 dBm + 6 dB - 142 dB + 0 dB = -86 dBm.

3. Häirintäsignaali on siis -86 dBm - (-101 dBm) = 15 dB voimakkaampaa kuin hyötysignaali. Häirintä on tehokasta.

4. Erilaisten tehoarvojen, yhteysetäisyyksien ja antennivahvistusten arviointi on jälleen vapaata ja yksinkertaista, mutta tulee muistaa, että kaavat antavat vain hyvin karkeita arvioita ja omaa toimintaa ei voi rakentaa ainakaan sellaisen tilanteen varaan, missä hyötysignaali- ja häirintätehot saavat saman suuruusluokan arvoja.

Hajaspektriviestijärjestelmien häirittävyyttä arvioitaessa tulee huomioida, että viesti-järjestelmän kannalta ideaalitilanteessa häiritsijä joutuu jakamaan häirintätehonsa koko hajaspektrijärjestelmän käyttämälle taajuuskaistalle. Vaikka hyötysignaali on levitetty samalle laajalle taajuuskaistalle, se kyetään kuitenkin kompressoimaan takaisin kapea-kaistaiseksi. Prosessoinnissa häirintäsignaali ei kompressoidu, joten häirintäteho heikkenee suhteessa hyötysignaalin tehoon suhteessa, jota kutsutaan hajaspektri-järjestelmän prosessointivahvistukseksi. Hajaspektritekniikka tuo siis häirinnältä lisä-suojaa sen prosessointivahvistuksen verran.

Yksinkertaisin hajaspektritekniikka on taajuuksien vaihtaminen niin nopeasti, ettei häiritsijä pysy perässä. Tällaisesta järjestelmästä käytetään nimitystä hyppivätaajuinen (FH, Frequency Hopping). Hyppivätaajuisen järjestelmän signaali on koko ajan kapeataajuinen, mutta kulloinkin käytettyä lähetystaajuutta vaihdetaan nopeasti laajalla hypintä(taajuus)kaistalla. Jos häirintäjärjestelmä ei kykene seuraamaan taajuuksien vaihtamista, sen on keskityttävä häiritsemään koko taajuuskaistaa tai osaa siitä.

Jälkimmäisessä tapauksessa osa järjestelmän käyttämistä kanavista jää kokonaan häiritsemättä. Ensin mainitussa tapauksessa keskimääräinen häirintäteho kutakin häirittävää kanavaa kohti laskee, koska häirintä jakautuu useille eri kanaville samanaikaisesti. Tällöin häirintä-signaalisuhde pienenee (desibeleissä ilmaistuna)[kk]:

$$J_{FH} = J - 10 \cdot \log_{10}\left(\frac{B_J}{B_S}\right)$$

missä $J_{FH}$ on hyötysignaaliin kohdistuva häirintäteho, $J$ on häirintäsignaaliteho vastaanottimessa koko taajuuskaistalla, $B_J$ häirintäsignaalin kaistanleveys (esimerkiksi koko taajuushypinnän kaista) ja $B_S$ taajuushyppivän radion hetkittäinen kaistanleveys (varsinaisen signaalin kaistanleveys).

Kun taajuushypinnän yksittäiset kanavat jakautuvat tasaisesti yhtenäiselle taajuuskaistalle ja häirintäjärjestelmä häiritsee koko kaistaa, kaavan suluissa oleva osuus yksinkertaistuu muotoon $B_J/B_S$ = *taajuuskanavien lukumäärä*. Tämä on erittäin hyvä nyrkkisääntö hyppivätaajuisen radion häirintäsietoisuutta arvioitaessa. Siten 1000 taajuutta käyttävän hyppivätaajuisen radion häirintä tehoaa vain tuhannesosan siitä kuinka hyvin sama häirintäteho tehoaisi pistetaajuiseen järjestelmään eli häirintä on $10 \cdot \log_{10}(1000) = 30$ dB tehottomampaa kuin perinteisen kapeakaistaisen radion häirintä (ks. myös Taulukon 3.2 arvoja).

Taajuushypintää monimutkaisempi, mutta vielä paremmin suojattu hajaspektritekniikka, on ns. suorahajotushajaspektrimenetelmä (DS/DSSS, Direct Sequence Spread Spectrum). Siinä kapeakaistainen hyötysignaali levitetään suoraan laajalle taajuuskaistalle[ll]. DS-signaalin häirintä on hankalaa jopa uusimmilla häirintäjärjestelmillä osin myös sen vuoksi, että DS-signaalin havaitseminenkin elektronisen tuen keinoin on hyvin hankalaa.

Häirintäjärjestelmän tehollinen (efektiivinen) häirintäteho DS-signaalia häirittäessä pienenee hajaspektrikaistan suhteessa informaatiokaistaan eli noudattaa kaavaa (desibelitehoyksiköissä)[mm]:

$$J_{DS} = J - 10 \cdot \log_{10}\left(\frac{B_{DS}}{B_S}\right)$$

missä $J_{DS}$ on varsinaiseen viestisignaaliin kohdistuva häirintäteho, $J$ aiempien kaavojen mukainen häirintäsignaaliteho vastaanottimessa, $B_{DS}$ se hajaspektriradion

---

[kk] Mikäli häirintäjärjestelmän käyttämä kaistanleveys on pienempi kuin taajuushypinnän kokonaiskaistanleveys, jää osa taajuushypyistä kokonaan häiritsemättä. Kaava kuvaa vain häirittyjen hyppyjen osuutta.

[ll] GPS-satelliitin signaalissa käytetään suorahajotusta. Yleisessä käytössä olevan signaalin prosessointivahvistus on 43 dB, sotilassignaalin tätäkin parempi. Signaalia on siten vaikea havaita tiedusteluvastaanottimella, joka ei tiedä tarkalleen millaiseen signaaliin lukittua.

[mm] Olettaen että koko häirintäteho osuu hajaspektriradion taajuuskaistalle.

lähetyskaistanleveys, jolle viestisisältö on levitetty ja $B_S$ varsinaisen informaatiokanavan kaistanleveys (vastaavan perinteisen kapeakaistaisen radion kaistanleveys). Kyseisen kaavan termi $B_{DS}/B_S$ (tai sen desibeliarvo) on nimeltään *prosessointivahvistus*, joka kuvaa hajaspektrijärjestelmän kykyä poistaa häirintää eli vahvistaa hyötysignaalia vastaanotossa kohinaan ja häirintään verrattuna.

DS-hajaspektritekniikan käyttö vaikeuttaa myös järjestelmän tiedusteltavuutta, koska lähetysteho on jakautunut suuremmalle alueelle spektrissä ja siten lähetteen tehotiheys on pienempi.

Taulukossa L3.3 on listattu erilaisia hyöty- ja häirintäsignaalin kaistanleveyksiä, joiden avulla hyppivätaajuisen järjestelmän häirintävaikutuksen heikentymistä voidaan arvioida. Samaa taulukkoa voidaan käyttää myös DS-järjestelmän prosessointivahvistuksen ja siten häirintävaikutuksen heikentymisen arviointiin.

| | $B_S$ 4 kHz | 25 kHz | 100 kHz | 500 kHz | 1 MHz | 2 MHz | 10 MHz | 50 MHz | 100 M |
|---|---|---|---|---|---|---|---|---|---|
| $B_J$ tai $B_{DS}$ 4 kHz | 0 | | | | | | | | |
| 25 kHz | 8 | 0 | | | | | | | |
| 100 kHz | 14 | 6 | 0 | | | | | | |
| 500 kHz | 21 | 13 | 7 | 0 | | | | | |
| 1 MHz | 24 | 16 | 10 | 3 | 0 | | | | |
| 2 MHz | 27 | 19 | 13 | 6 | 3 | 0 | | | |
| 10 MHz | 34 | 26 | 20 | 13 | 10 | 7 | 0 | | |
| 50 MHz | 41 | 33 | 27 | 20 | 17 | 14 | 7 | 0 | |
| 100 MHz | 44 | 36 | 30 | 23 | 20 | 17 | 10 | 3 | 0 |

**Taulukko L3.3. Hyppivätaajuisen viestijärjestelmän saavuttama häirintä-signaalisuhteen parannus (siis pinennys) desibeleinä, mikäli häirintä kohdistuu vähintään koko käytetylle kokonaistaajuuskaistalle. $B_S$ on taajuushyppivän radion hetkellinen kaistanleveys (informaation kaistanleveys; vastaavan perinteisen kapeakaistaisen radion kaistanleveys) ja $B_J$ on häirintäsignaalin kaistanleveys. Jos siis esim. 4 kHz:n puhesignaalia hypytetään 1 MHz:n kaistalla, joksi myös häirintäjärjestelmä optimoi häirintäkaistanleveytensä, pienenee häirintä-signaalisuhde 24 dB. Samaa taulukkoa voi myös käyttää suorahajotushajaspektrijärjestelmän prosessointivahvistuksen ja häirintä-signaalisuhteen muutoksen arviointiin.**

## Esimerkki L3.4

Mikäli kenttäradiossa käytetään taajuushypytystä, jota häirintälähetin ei kykene seuraamaan, se joutuu jakamaan häirintätehonsa tasaisesti koko hypintäkaistalle. Tällöin häirintätehon ja sen vaikutuksen heikkeneminen arvioidaan seuraavasti: Tarkastellaan edellisen esimerkin 5 W:n tehoisen 5 km:n kenttäradioyhteyden häiritsemistä taktisella häirintälavetilta 20 km:n päästä, kun kenttäradio hypyttää lähetettään (25 kHz puhekaista) 1 MHz:n taajuusalueella.

1. Lasketaan hyötysignaaliteho vastaanottimessa edellisen esimerkin mukaisesti kaavalla

   $S = P_{LS} + G_{LS} - L_S + G_{VS}$ = 37 dBm + 0 dB - 138 dB + 0 dB = -101 dBm.

2. Lasketaan vastaanottimeen tuleva häirintäteho koko taajuuskaistalle (kapeakaistaisen perinteisen vastaanottimen tapauksessa) edellisen esimerkin mukaisesti kaavalla

   $J = P_{LJ} + G_{LJ} - L_J + G_{VJ}$ = 50 dBm + 6 dB - 142 dB + 0 dB = -86 dBm.

3. Lasketaan häirintälähettimen teho hyötysignaalitaajuudella eli vastaanottimessa läpi pääsevä häirintäteho, kun häirintälähetin joutuu jakamaan tehonsa koko taajuusalueelle, kaavalla

   $J_{FH} = J - 10 \times \log_{10}(B_J/B_S)$:

   - Häirintäteho koko taajuuskaistalla (perinteisen kapeakaistaisen radion tapauksessa) saatiin edellä $J$ = -86 dBm.
   - Taajuushypytyksen kokonaistaajuuskaista on $B_J$ = 1 MHz = 1000 kHz.
   - Lähetteen hetkellinen kaistanleveys eli varsinaisen signaalin kaistanleveys, on $B_S$ = 25 kHz.
   - Tästä saadaan $J_{FH}$ = -86 dBm - 10 x $\log_{10}$(1000/25) = -102 dBm. Tätä arvoa verrataan kohdan 1 hyötysignaalitehoon.

4. Hyötysignaaliteho ja hyppivätaajuisen lähetteen hetkelliselle taajuuskaistalle osuva häirintäteho ovat käytännössä samansuuruiset (-101 dBm ja -102 dBm). Esim. sähkötys ja AM-puhelähete saattaisivat hyvinkin päästä läpi, mutta herkällä digitaalilähetteellä olisi ongelmia. Pienellä suuntaavuudella antennissa tai maastoesteitä hyödyntämällä tilanne voitaisiin helposti korjata kenttäradion kannalta kuntoon.

5. Pohditaan tilanne vielä huolella: jakaako häiritsijä tehonsa koko kaistalle? Mahdollisuuksia on useita:

   - Häiritsijällä onkin niin moderni häirintäjärjestelmä ja tilannegeometria on sellainen, että häiritsijä kykenee seuraamaan lähetettä hyppy hypyltä. Tällöin edellä käsitelty ei päde, vaan tilanne vastaa kapeakaistaisen radion häirintää.
   - Häiritsijä on jostain syystä jakanut häirintätehoaan kenttäradion taajuuskaistaa laajemmalle. Tällöin tilanne on kenttäradiolle vielä edullisempi: häiritsijä hukkaa tehoaan, ja $B_J$:n kohdalla kaavoissa käytetään häiritsijän käyttämää kaistanleveyttä.
   - Häiritsijä ei jaa häirintätehoaan koko kenttäradion käyttämälle kaistalle. Tällöin osaa taajuushypyistä häiritään, osaa ei. Tässä kuvatulla tavalla arvioidaan, kykeneekö häiritsijä estämään häiritsemiensä taajuuksien käytön ($B_J$:n kohdalla kaavoissa käytetään häiritsijän käyttämää kaistanleveyttä). Mikäli kykenee, tulee arvioida miten kyseisten

hyppyjen estyminen vaikuttaa tietoliikenteeseen. Häiritsijä saattaa esim. tietää, että digitaalitiedonsiirto estyy täysin jo kun 20% hypyistä häiritään, ja saattaa optimoida häirintätehonsa vain tähän osaan taajuuksista.

Vastaavasti, kuten liitteessä 2 korostettiin, jälleen on muistettava, että radioaaltojen eteneminen ja häirinnän tehokkuuden arviointi on olennaisesti tässä liitteessä kuvattua monimutkaisempi ilmiömaailma. Kenttäolosuhteita varten on kuitenkin hyödyllistä painaa mieleen muutamia perustilanteita, joiden avulla häirittävyyttä voi arvioita.

## Tutkajärjestelmien suojaaminen

Tutkajärjestelmien häirittävyyden arviointi on monimutkaisempi kysymys kuin viestijärjestelmien, sillä häirittävyyteen vaikuttaa myös tutkamaalin koko (tutkapoikkipinta) sekä tutkan signaalinkäsittely. Esimerkiksi pulssidopplertutkat voivat suodattaa valtaosan kohinahäirintätehosta pois. Nykyaikaisten tutkien häirinnänväistömenetelmät ovat niin kehittyneitä, että tutkien häiritsemisen edellyttää yleensä harhauttavan häirinnän käyttämistä. Liitteessä 5 on käsitelty tutkan häirintä-signaali-suhdetta ja häirintään liittyviä kaavoja. Aiemman viestijärjestelmin käsittelyn mukaisesti seuraavassa esitetään karkea menetelmä tutkien häirittävyyden arvioimiseksi.

Tutkan hyötysignaali käyttäytyy toisin kuin viestijärjestelmässä, koska tutkan signaali ensin vaimenee edetessään tutkalta kohti maalia, josta se heijastuu tai siroaa heikkona kaikuna ja vaimenee toisen kerran matkallaan takaisin tutkaa kohti.

Tutkapulssin vastaanottotehoksi saadaan vapaassa tilassa ja hiukan yksinkertaistaen *desibeleinä:*

$$S = P_{LS} + 2 \cdot G + 10 \cdot \log_{10}(s) - 20 \cdot \log_{10}(f) - 40 \cdot \log_{10}(R_{MAALI}) - 163$$

missä $P_{LS}$ on tutkan lähetysteho (yksiköissä dBm), $G$ tutkan antennivahvistus pääkeilan suuntaan (dB), $\sigma$ tutkamaalin poikkipinta ($m^2$), $f$ tutkan taajuus (GHz) ja $R_{MAALI}$ maalin etäisyys tutkasta (km).

Häirintäsignaalin teho $J$ lasketaan kuten edellä viestijärjestelmien yhteydessä kuvattiin.

Taulukoissa L3.4 ja L3.5 on esitetty esimerkkejä hyöty- ja häirintäsignaaleiden tehoista tutkan vastaanottimessa. Niiden avulla häirinnän tehokkuutta voidaan arvioida erilaisilla maalin ja häirintälähettimen etäisyyksillä[67]. Tässä yhteydessä on muistettava, että tutkahäirintä kohdistuu tutkaan usein sen antennin sivukeilasta. Tällöin häirintätehosta tulee vähentää tutkan antennivahvistus kyseiseen suuntaan. Yleensä laskuissa käytetään keskimääräistä sivukeilatasoa, jolloin häirittävyydestäkin saadaan keskimääräinen arvio.

| | 1 km | 5 km | 10 km | 50 km | 100km | 200km | 500km |
|---|---|---|---|---|---|---|---|
| **Suuri ilmavalvontatutka (*f*=3 GHz, $P_{LS}$=2 MW, *G*=40 dB)** | | | | | | | |
| - Häivelentokone (s =0,001 $m^2$) | -30 | -58 | -70 | -98 | -110 | -122 | -138 |
| - Hävittäjä/rynnäkkökone (s =1 $m^2$) | 0 | -28 | -40 | -68 | -80 | -92 | -108 |
| - Iso pommikone (s =100 $m^2$) | 20 | -8 | -20 | -48 | -60 | -72 | -88 |
| **Pieni ilmavalvontatutka (*f*=5 GHz, $P_{LS}$=20 kW, *G*=25 dB)** | | | | | | | |
| - Häivelentokone (s =0,001 $m^2$) | -84 | -112 | -124 | -152 | -164 | -176 | -192 |
| - Hävittäjä/rynnäkkökone (s =1 $m^2$) | -54 | -82 | -94 | -122 | -134 | -146 | -162 |
| - Iso pommikone (s =100 $m^2$) | -34 | -62 | -74 | -102 | -114 | -126 | -142 |
| **Hävittäjätutka (*f*=10 GHz, $P_{LS}$=10 kW, *G*=30 dB)** | | | | | | | |
| - Häivelentokone (s =0,001 $m^2$) | -83 | -111 | -123 | -151 | -163 | -175 | -191 |
| - Hävittäjä/rynnäkkökone (s =1 $m^2$) | -53 | -81 | -93 | -121 | -133 | -145 | -161 |
| - Iso pommikone (s =100 $m^2$) | -33 | -61 | -73 | -101 | -113 | -125 | -141 |

**Taulukko L3.4 Tutkajärjestelmien kaikupulssien tehoja dBm-yksiköissä vastaanottimessa erilaisilla mielivaltaisilla, mutta suuruusluokiltaan realistisilla, toimintaparametreilla ja tutkamaalin etäisyyksillä. Vertaa näitä arvoja Taulukon L3.5 häirintätehoihin samoissa vastaanottimissa. Huomaa, että maalin etäisyyden kaksinkertaistuminen pienentää tutkakaiun tehoa 12 dB, kun häirintäsignaaliteho pienenee vastaavasti vain 6 dB.**

Vertailemalla taulukossa L3.4 esitettyjä hyötysignaalitasoja taulukon L3.5 häirintäsignaalien tehotasoihin voidaan arvioida häirinnän tehokkuutta erilaisissa tilanteissa, täsmälleen kuten aiemmissa viestijärjestelmien esimerkeistä kuvattiin. Taulukoista havaitaan, että tutkan on hyvin vaikeaa pärjätä tehokilpailussa häirintälähettimelle. Tämä pätee erityisesti häiritsijän vaikuttaessa tutkan pääkeilassa eli silloin kun häirintä toteutetaan omasuoja- tai saattohäirintänä.

## Esimerkki L3.5

Tarkastellaan tilannetta, jossa tutkaa lähestyy ilmapuolustuksen lamautusosasto, jonka lähestyminen suojataan a) osaston mukana lentävällä saattohäirintäkoneella (4 kW häirintälähetin liitettynä 6 dB antenniin), b) 150 km etäisyydellä toimivalla taustahäirintäkoneella (100 kW häirintälähetin liitettynä 15 dB antenniin) ja 3) lähihäirintälennokilla 2 km päässä tutkasta (25 W lähetin ja 3 dB antenni). Esimerkkiä voidaan tarkastella taulukoiden L3.4 ja L3.5 avulla. Havainnollisuuden vuoksi näissä taulukoissa esitetty informaatio on piirretty kuvaksi L3.6, jossa esitetään esimerkin tutkan signaalin suhde häirintäsignaaliin. Kuvasta nähdään, että tutkan signaali ylittää häirintäsignaalin taustahäirintälähettimellä suojatussa tapauksessa noin kahden kilometrin päässä ja häirintälennokilla suojatussa tapauksessa reilun kolmen kilometrin päässä. Saattohäirintälähettimen teho riittää pitämään tutkakaiun häirintäsignaalia pienempänä aivan tutkan päälle asti.

| | 1 km | 5 km | 10 km | 50 km | 100km | 200km | 500km |
|---|---|---|---|---|---|---|---|
| **Omasuojahäirintä ($P_{LJ}$=1 kW, $G_{LJ}$=3 dB)** | | | | | | | |
| - Suuri ilmavalvontatutka | 1 | -13 | -19 | -33 | -39 | -45 | -53 |
| - Pieni ilmavalvontatutka | -18 | -32 | -38 | -52 | -58 | -64 | -72 |
| - Hävittäjätutka | -19 | -33 | -39 | -53 | -59 | -65 | -73 |
| **Saattohäirintä ($P_{LJ}$=4 kW, $G_{LJ}$=6 dB)** | | | | | | | |
| - Suuri ilmavalvontatutka | 10 | -4 | -10 | -24 | -30 | -36 | -44 |
| - Pieni ilmavalvontatutka | -9 | -23 | -29 | -43 | -49 | -55 | -63 |
| - Hävittäjätutka | -10 | -24 | -30 | -44 | -50 | -56 | -64 |
| **Taustahäirintä ($P_{LJ}$=100 kW, $G_{LJ}$=15 dB)** | | | | | | | |
| - Suuri ilmavalvontatutka | 33 | 19 | 13 | -1 | -7 | -13 | -21 |
| - Pieni ilmavalvontatutka | 14 | 0 | -6 | -20 | -26 | -32 | -40 |
| - Hävittäjätutka | 13 | -1 | -7 | -21 | -27 | -33 | -41 |

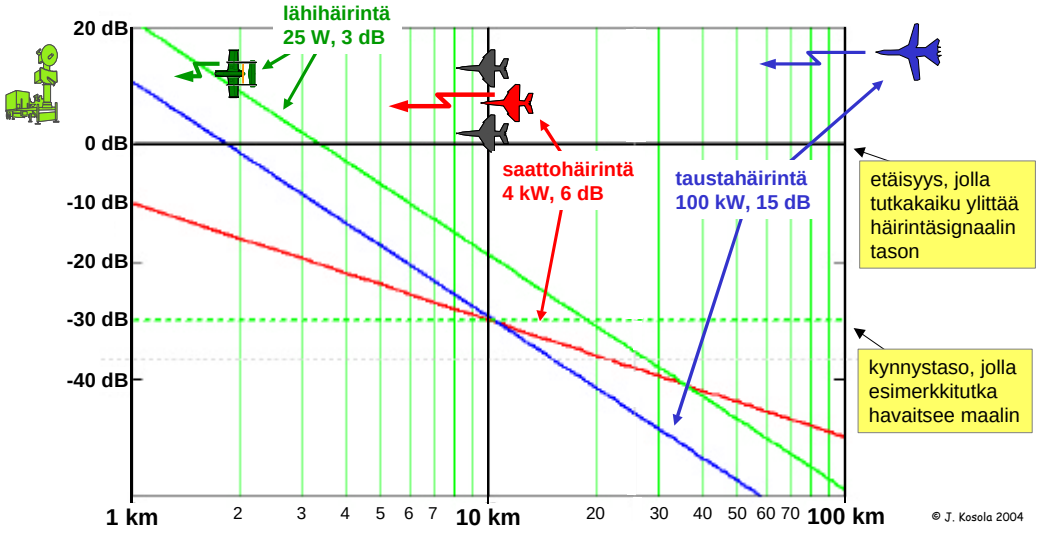
**Taulukko L3.5. Erilaisten mielivaltaisten, mutta suuruusluokiltaan realististen, häirintäjärjestelmien aikaansaamia häirintätehoja dBm-mittayksiköissä taulukon L3.4 tutkajärjestelmiin. Taulukossa oletetaan, että häirintäjärjestelmä toimii tutkan pääkeilassa, joten tilanne vastaa omasuoja- tai saattohäirintää. Sivukeilahäirinnän tapauksessa tehotasosta tulee vähentää tutkan sivukeilataso kyseiseen suuntaan. Myös tutkan häirinnänväistöominaisuudet ja etenkin pulssidopplertutkan käyttämä pulssien integrointi vaikuttavat tilanteeseen hyvin huomattavasti.**

Tutkalle epäedullisen tilannegeometrian vuoksi sotilastutkajärjestelmissä käytetään monimutkaisia häirinnänväistömenetelmiä, eikä edellä kuvattu yksinkertainen teho-tarkastelu riitä todellisten sotilastutkajärjestelmien suorituskyvyn arviointiin. Tutka kykenee integroimaan useita tutkapulsseja ja siten yhdistämään maalista heijastuvien useiden pulssien energian. Lisäksi tutkavastaanotin on sovitettu odottamaan tietyn tyyppistä kaikua, joka perustuu tutkan itsensä lähettämään pulssiin. Tutka pyrkii maksimoimaan odotetuista kaiuista vastaan otettavan energian ja minimoimaan muun kaltaisista pulsseista tulevan energian. Siten tutka hylkää osan vastaanottamastaan häirintäsignaalin energiasta. Näin aikaan saatava parannus voi olla useita kymmeniä desibelejä.

## Esimerkki L3.6

Edellistä esimerkkiä jatkaaksemme voidaan arvioida *esimerkiksi*, että tutka kykenee erilaisin häirinnänväistökeinoin parantamaan (siis vähentämään) häirintä-signaalisuhdetta 30 dB verran. Tätä -30 dB havaitsemiskynnystä esittää kuvan L3.6 vaakasuorassa oleva katkoviiva. Sen perusteella havaitaan 30 dB häirinnänväistöön kykenevän tutkan havaitsevan

- saatto- tai taustahäirinnällä suojatun maalin 10 km etäisyydeltä
- lähihäirintälennokilla suojatun maalin hieman alle 20 km etäisyydeltä.




**Kuva L3.6: Esimerkkitutkan hyötysignaalin ja häirintätehon suhde maalin ollessa eri etäisyyksillä, muutamalle eri häirintäjärjestelmälle. Kuvaan on merkitty tutkan läpipolttoetäisyys (0 dB signaali-häirintäsuhde) ja havaitsemisetäisyys häirinnänväistötoimenpiteiden johdosta (-30 dB taso vihreällä katkoviivalla), kun esimerkinomaista kaukovalvontatutkaa häiritään 100 kW taustahäirintäkoneella 150 km etäisyydeltä, osaston mukana lentävällä 4 kW saattohäirintäkoneella ja 25 W häirintälennokilla 2 km etäisyydellä tutkasta.**

Toisaalta moderni häirintäjärjestelmä kykenee väistämään tutkan häirinnänväistöominaisuuksia, ja tilanne palaa jälleen tehokamppailuksi, kunnes tutkajärjestelmään kehitetään uusia häirinnänväistömenetelmiä. Näiden kuvaaminen rajautuu tämän kirjan aihepiirin ulkopuolelle. Tehotasojen tarkastelu antaa kuitenkin käsityksen häirintään liittyvien etäisyyksien suuruusluokista ja tehojen suhteista. Edellä kuvattu esimerkki tuo selkeästi esiin elektronisen häirinnän merkityksen tutkaverkon lamauttamisessa. Vaikka häirintäteho olisi pienempikin ja tutkalla olisi käytettävissään tässä esimerkissä esitettyjä tehokkaampia häirinnänväistömenetelmiä, romahtaa yksittäisen tutkan suorituskyky häirinnän vuoksi. Nämä tutkat kykenevät kuitenkin määrittämään häirintälähetteen tulosuunnan. Lisäksi tutkat, jotka toimivat häirintälähettimen toimintasuunnan suhteen sivussa, voivat kyetä havaitsemaan maalit. Siten integroitu ilmapuolustusjärjestelmä, jossa samaa maalia voidaan seurata useilla eri tutkilla, voi kyetä muodostamaan ilmatilannekuvan, vaikka sen yksittäiset tutkat häirittäisiinkin lähes sokeiksi. Tämä onkin yksi syy sille, miksi ilmapuolustusjärjestelmän lamauttamisessa pyritään pilkkomaan integroitu tutkajärjestelmä toisistaan erillään toimiviksi yksittäisiksi tutkiksi lamauttamalla tai tuhoamalla sen viesti- ja johtamisjärjestelmä.

# LIITE 4: RADIOTAAJUISET ASEET

Radiotaajuiset aseet ovat kokonaan uusi asekategoria, jossa asevaikutus ei perustu minkäänlaiseen fyysiseen projektiiliin, vaan sähkömagneettiseen säteilyyn. Radiotaajuiset aseet kohdentavat maalina oleviin järjestelmiin niin suuren sähkömagneettisen energian, että maalissa oleva elektroniikka tuhoutuu tai vaurioituu. Radiotaajuista energiaa käytetään suurtehomikroaaltoaseessa (HPM, High-Power Microwave) sekä sähkömagneettiseen pulssiin (EMP, Electromagnetic Pulse) perustuvassa EMP-aseessa.

Radiotaajuisilla aseilla on useita etuja verrattuna konventionaalisiin asejärjestelmiin:

- valon nopeus "projektiilin" lentonopeutena; välitön vaikutus maaliin
- suora lentorata: yksinkertainen seurantajärjestelmä; ennakkoa ei tarvita
- näkymätön ja äänetön vaikutuskeino; ei paljastu helposti, joten kohde ei osaa suojautua eikä käynnistää vastatoimenpiteitä jos ase ei tehoa tai sillä ammutaan ohi.
- periaatteessa ehtymätön "lipas"
- kyky vaikuttaa useisiin maaleihin erittäin lyhyessä ajassa; kyky torjua saturaatiohyökkäyksiä
- vaikutuskyky nopeisiin ja liikehtimiskykyisiin maaleihin, kuten lentokoneisiin ja ohjuksiin
- epäherkkä aktiivisille elektronisille vastatoimenpiteille
- asevaikutuksen kustannus maalia kohti erittäin pieni

Toisaalta edellä lueteltujen etujen lisäksi radiotaajuisten aseiden heikkouksina voidaan pitää muun muassa seuraavia ominaisuuksia:

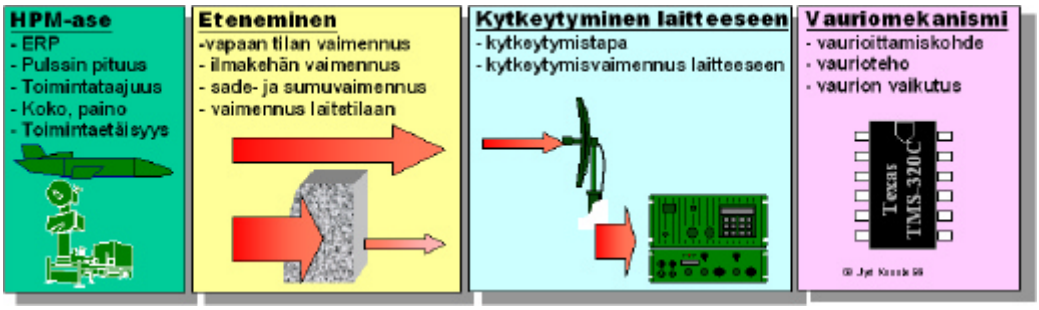
- maalin on oltava näköyhteysreitillä
- aseen teho riippuu säästä pitkillä etäisyyksillä
- vaikutus maaliin on monimutkainen ja riippuu maalin elektronisen suojautumisen ominaisuuksista
- asevaikutuksen todentaminen saattaa olla vaikeata, sillä osumaa ja maalin elektroniikan lamautumista ei välttämättä kyetä päättelemään päällepäin edes lähietäisyydeltä
- teknologia ei vielä (2004) ole kypsää, joten aseiden koko ja paino ovat vielä suuria ja niiden käytettävyys on epävarma.

Radiotaajuisten aseiden ominaisuuksien vuoksi niitä pidetään seuraavan merkittävän sodankäynnin murroksen mahdollisena synnyttäjänä, sillä niillä on potentiaalia horjuttaa koko sitä teknologista perustaa, jolle nykyaikainen sodankäynti perustuu.

Lisäksi niillä kyetään vakavasti uhkaamaan länsimaisen informaatioyhteiskunnan perusinfrastruktuuria[68].

Suurtehomikroaaltoaseessa radiotaajuinen pulssi johdetaan lähetysantenniin, josta se etenee maaliin sähkömagneettisena säteilynä ja tunkeutuu ajoneuvojen, konttien ja laitteiden sisälle ovien, luukkujen ja läpivientien raoista sekä indusoituu kohdejärjestelmän antenneihin ja metallijohtimiin ja tunkeutuu kaapeliyhteyksiä pitkin laitteistoon.

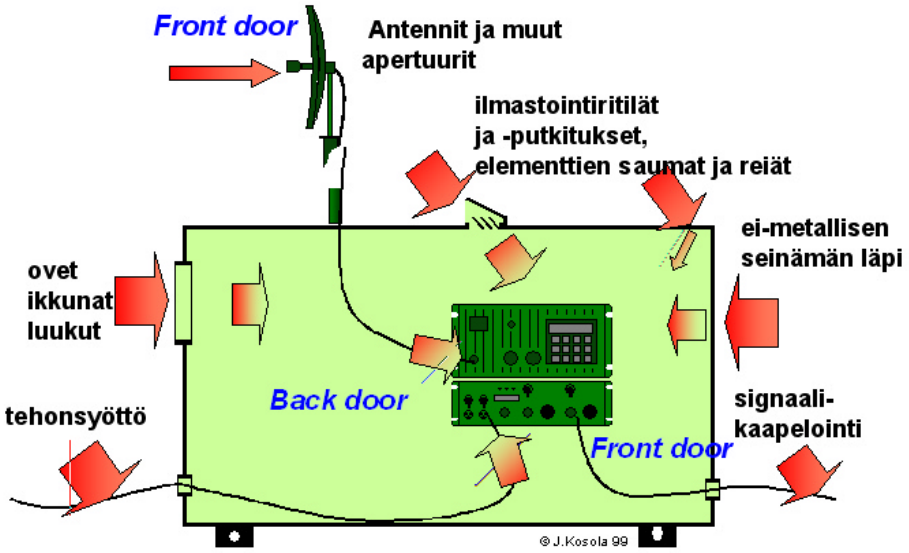
HPM-aseen uhka perustuu suurelta osin sen suureen toimintataajuuteen, joka mahdollistaa lyhyiden suurienergisten pulssien muodostamisen sekä säteilyenergian tunkeutumisen kohdelaitteisiin, jotka on suojattu matalampitaajuiselta säteilyltä, esimerkiksi EMP-suojauksella.




**Kuva L4.1: Radiotaajuisen aseen toimintaan vaikuttavat tekijät.**

HPM-ase voi olla esimerkiksi terroristien tai erikoisjoukkojen käyttöön tarkoitettu HPM-salkkupommi, risteilyohjuksen tms. maalin läheisyyteen toimitettavan aseen taistelukärki tai lavettiin kiinteästi asennettu HPM-ase tai -omasuojajärjestelmä. Salkkupommi on pienimmillään attaseasalkun kokoinen ja suurimmillaan umpipakettiauton tavaratilaan mahtuva ase. Risteilyohjuksen HPM-taistelukärki asennetaan konventionaalisen taistelukärjen tilalle. Sen kantama on jonkin verran HPM-salkkuaseen kantamaa suurempi, mutta kantamaa rajoittaa ohjuksen liikkeestä ja suunnistamisesta johtuva tähtäyksen epätarkkuus, joka rajoittaa aseen tehollista kantamaa.

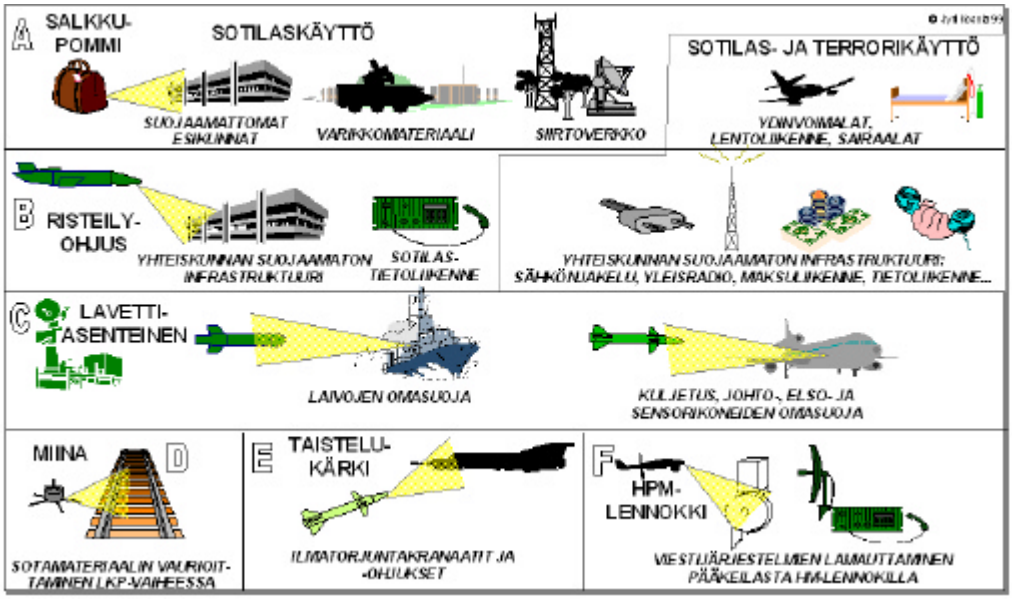
Laivaan, lentokoneeseen tai ajoneuvoon asennettavassa HPM-aseessa voidaan käyttää suurempia antennirakennelmia kuin edellä mainituissa aseissa. Lisäksi tällaisessa aseessa pulssi muodostetaan sähköenergialla eikä räjäyttämällä, joten aseella voidaan ampua useita ’laukauksia’ – esimerkiksi 100-200 pulssia sekunnin aikana, jonka jälkeen asetta on jäähdytettävä joitakin sekunteja ennen uuden pulssisarjan ampumista. Tällaisen aseen ja sen teholähteiden paino ja koko sekä mikroaaltojen etenemisominaisuudet rajoittanevat sen käytön lähinnä laivojen ja lentokoneiden omasuojajärjestelmiin sekä mahdollisesti lentokoneeseen asennettuun hyökkäykselliseen järjestelmään. Maahan sijoitettuna ase sopisi parhaiten lentokoneiden ja älykkäiden ammusten torjuntaan lähietäisyydeltä.




**Kuva L4.2: Radiotaajuisen säteilyn tunkeutumisreittejä laitetiloihin ja laitteisiin. ”Front door” tarkoittaa niitä reittejä, jotka on itse järjestelmässäkin suunniteltu radiotaajuisen signaalin kulkureiteiksi (antennit, signaalikaapelit yms.). ”Back door” ovat erilaiset järjestelmän sekalaiset luukut, resonoivat johtimet yms., joita pitkin korkeatehoinen mikroaaltopulssi voi myös tunkeutua laitteeseen.**

HPM-aseen lyhyt kantama ja vaikutuksen suunnattavuus pienentää sen käyttökynnystä. EMP-ase vaikuttaa kaikkiin ympäristön elektronisiin järjestelmiin, myös kriittisiin siviilikohteisiin, kun taas HPM-aseella voidaan kohteiksi valita vain halutut sotilas-järjestelmät.

Suojautuminen radiotaajuisia aseita vastaan alkaa uhka-arvion laadinnasta. Siinä on arvioitava mitä puolustajan järjestelmiä vastaan käytettäisiin nimenomaan radio-taajuisia aseita eikä esimerkiksi konventionaalista asevaikutusta. Tällöin on myös arvioitava minkä tyyppistä asetta hyökkäyksessä käytettäisiin. Ensin siis määritellään toimintaympäristön sähkömagneettinen uhka. Tämän perusteella voidaan joko määritellä laitteilta edellytettävä sähkömagneettinen suojataso käyttäen hyväksi tietoja tilojen ja asennusten suojatasoista - tai voidaan määrittää vaatimukset laitetiloille ja laiteasennuksille niihin sijoitettavien laitteiden ympäristönkestokyvyn perusteella. Laitteiden sietokyky määräytyy käytännössä noudatettavan teknologiapolitiikan mukaan; kaupallisten laitteiden sietokynnys on matalampi kuin sotilaselektroniikan. Päähuomio tulee kiinnittää laitetilojen ja järjestelmäasennusten suojatasoon ja sähkömagneettisesti herkkien järjestelmien toimintaperiaatteeseen ja rakenteeseen. Sähkömagneettisesti herkillä järjestelmillä tarkoitetaan tässä sellaisia järjestelmiä, joiden toimintaperiaatteeseen kuuluu sähkömagneettisen energian tehokas kytkeminen ilmasta laitteisiin, kuten radiolaitteet, satelliitti- ja radiopaikantamislaitteet sekä tutkat ja elektronisen tiedustelun sensorit. Näissä joudutaan käyttämään erilaisia teknisiä suojautumiskeinoja.




**Kuva L4.3: HPM-aseen mahdollisia käyttökohteita ja erilaisia asetyyppejä.**

Yleiskäyttöisenä suojautumiskeinona toimii järjestelmien sijoittaminen siten, ettei vastustaja kykene vaikuttamaan niihin HPM-aseella, esimerkiksi sijoittamalla ne metsän, rakennusten, maastoesteiden yms. suojaan potentiaalisimmalta uhkasuunnalta, estämällä vastustajan pääsy sille alueelle, jolta salkku- ja pakettiautoaseet muodostavat uhan ja sijoittamalla kriittisimmät järjestelmät joko maanalaisiin tiloihin tai rakennusten keskelle.

Radiotaajuisista aseista ja erityisesti suurtehomikroaaltoaseesta lisämateriaalia voi lukea MpKK:n julkaisuista *Digitaalinen Taistelukenttä* sekä *Suurtehomikroaaltoase ja perusteet siltä suojautumiselle*[69].

# LIITE 5: ELEKTRONISEN SODANKÄYNNIN TEKNIIKKAAN LIITTYVIÄ KÄSITTEITÄ

Tässä liitteessä käsitellään joitakin elektronisen sodankäynnin keskeisimpiä fysikaalisia ja matemaattisia käsitteitä konkreettisella ja käytännöllisellä tasolla. Liitteessä esitettyjen lainalaisuuksien ymmärtäminen on tärkeää, mikäli halutaan ymmärtää elektronisen sodankäynnin järjestelmien suorituskykyä tai ELSO:n vaikutusta sen kohdejärjestelmiin. Näitä käsitteitä syvennetään myös liitteissä 2 ja 3 hiukan eri tarkastelunäkökulmista.

## Desibeli – joustava tapa käsitellä tehoyksiköitä

Elektronisessa sodankäynnissä asioita ilmaistaan usein desibeleinä. Desibeleillä on kaksi hyödyllistä ominaisuutta:

1. Hyvin pieniä ja suuria lukuja voidaan ilmaista helposti hahmotettavina luonnollisen oloisina numeroina. Esimerkiksi alue -50…+50 dB kattaa lineaarisilla ”tavallisilla” yksiköillä alueen 0,00001 – 100.000.

2. Laskutoimitukset ovat yksinkertaisia. Esimerkiksi lineaaristen yksiköiden tulo yksinkertaistuu desibeleinä yhteenlaskuksi, jakolasku vähennyslaskuksi ja potenssiin korotus kertolaskuksi. Desibeleillä voidaan siten tehdä elektronisessa sodankäynnissä tarvittavia laskelmia jopa päässälaskuna. Esimerkiksi lineaarisilla luvuilla tehtävä lasku:

   20 000 x 80 000 / 100 000 000 000 000 = 0,000016

   on vaikea laskea päässä, mutta muutettuna logaritmeiksi, sama lasku on helppo laskea myös päässä tai ruutupaperilla:

   43 + 49 - 140 = -48

Desibelien ja lineaaristen lukujen välillä liikutaan seuraavilla yhtälöillä:

$$P_{dB} = 10 \cdot \log_{10} \frac{P}{P_{VERT}}$$

$$P = P_{VERT} \cdot 10^{\frac{P_{dB}}{10}}$$

missä $P_{dB}$ on teho desibeleinä ja $P$ sama teho lineaarisissa yksiköissä. $P_{VERT}$ on vertailuteho, mihin kyseistä tehoa kyseisessä tilanteessa verrataan.

Perussäännöt

| lineaariset luvut | | desibelit |
|---|---|---|
| 0,01 | = | -20 dB |
| 0,1 | = | -10 dB |
| 1 | = | 0 dB |
| 2 | = | 3 dB |
| 10 | = | 10 dB |
| 100 | = | 20 dB |
| 1000 | = | 30 dB |
| kertolasku | = | yhteenlasku |
| jakolasku | = | vähennyslasku |
| x 2 | = | + 3 |
| x 10 | = | + 10 |
| / 2 | = | - 3 |
| / 10 | = | - 10 |

Desibelejä käytetään ilmaisemaan *tehosuureita*, kuten signaalitehoa, sekä tehosuureisiin liittyviä vahvistus- ja vaimennustekijöitä. Desibelit ovat aina *vertailu-yksiköitä* – tietty desibelilukema ei itsessään kerro mitään tehoarvoa, vaan ainoastaan tarkasteltavan asian voimakkuuden verrattuna johonkin tehoarvoon. ELSO-laskuissa desibelejä käytetään ilmaisemaan sähkömagneettisen säteilyn signaalitehoja. Koska desibeli on vertailuyksikkö, sidotaan tehoarvo vertailtavaan tehotasoon ilmaisemalla myös se teholuku, johon signaalia verrataan. Yleisesti käytetyt yksiköt ovat:

- dBW – vertailutehona 1 W
- dBm – vertailutehona 1 mW = 0,001 W = -30 dBW

Esimerkkeinä joitakin signaalitehoarvoja eri tavoilla ilmaistuna:

- 0,0001 W = -40 dBW = -10 dBm
- 0,001 W = -30 dBW = 0 dBm
- 0,01 W = -20 dBW = 10 dBm
- 0,1 W = -10 dBW = 20 dBm
- 1 W = 0 dBW = 30 dBm
- 10 W = 10 dBW = 40 dBm
- 100 W = 20 dBW = 50 dBm

Desibeliyksiköitä käytetään kuvaamaan myös tehosuureiden muutoksia, esimerkiksi signaalin voimistumista vahvistimessa tai antennissa, tai signaalin vaimenemista sen edetessä. Esimerkiksi vahvistus 30 dB tarkoittaa signaalitehon kasvamista tuhatkertaiseksi ja etenemisvaimennus 90 dB signaalin heikentymistä yhteen miljardisosaan (kumpikin realistisia arvoja).

Esimerkiksi 10 watin lähettimen lähetysteho on desibeleinä 10 x log(10) = 10 dBW ja desibelimilliwatteina esitettynä 10 + 30 = 40 dBm. Jos lähetin varustetaan 13 dB

antennilla, se antaa antennin pääkeilan suuntaan 40 dBm + 13 dB = 53 dBm efektiivisen lähetystehon (EIRP, Equivalent Isotropic Radiated Power). Jos tämä säteilyteho vaimenee 46 desibeliä edetessään vastaanottimelle, vastaanottimelle saadaan teho 53 dBm - 46 dB = 7 dBm.

## Taajuus ja aallonpituus

Radioaaltojen käyttäytyminen riippuu voimakkaasti lähetystaajuudesta. Monesti kuitenkin puhutaan aallonpituudesta, joka tietyissä tilanteissa on havainnollisempi suure. Näiden välillä liikutaan seuraavilla kaavoilla:

$$f = \frac{3 \cdot 10^8 \text{ m/s}}{l} \Leftrightarrow l = \frac{3 \cdot 10^8 \text{ m/s}}{f}$$

missä $f$ on taajuus ja $l$ aallonpituus. Käytännöllisinä pikakaavoina voi käyttää seuraavia:

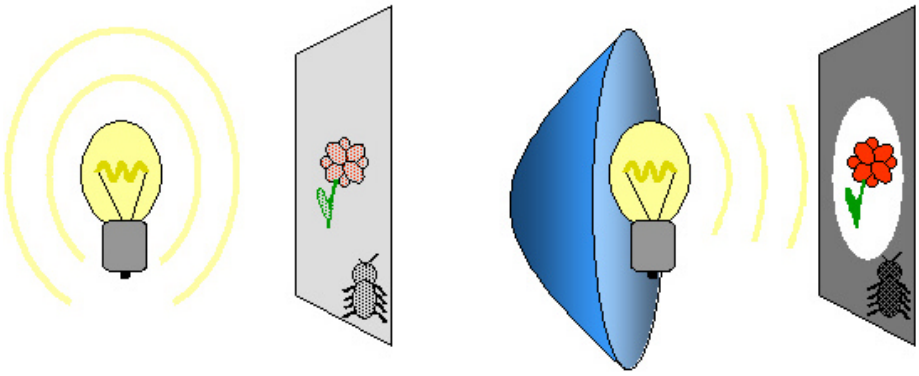
$$f_{\text{GHz}} = \frac{30}{l_{\text{cm}}} \Leftrightarrow l_{\text{cm}} = \frac{30}{f_{\text{GHz}}}$$

missä $f_{GHz}$ on taajuus gigahertseinä ja $l_{\text{cm}}$ aallonpituus senttimetreinä. Esimerkiksi taajuutta 1 GHz vastaa aallonpituus 30 / 1 = 30 cm ja taajuutta 10 GHz vastaa aallonpituus 30 / 10 = 3 cm.

## Antenni – keskeinen järjestelmän suorituskykyyn vaikuttava tekijä

Antenni on ELSO-järjestelmän ja ELSO:n kohdejärjestelmän keskeisimpiä suorituskykyyn vaikuttavia komponentteja. Antenni tehdään aina tietylle *taajuusalueelle*, jolle sen suorituskyky optimoidaan. Elektronisen sodankäynnin järjestelmissä antennin *kaistanleveys* (taajuusalueet, joilla se toimii) pyritään saamaan usein mahdollisimman suureksi (*laajakaistaiset antennit)*, jotta samalla antennilla voidaan tiedustella tai häiritä mahdollisimman monella eri taajuudella toimivia kohdejärjestelmiä. Elektronisen sodankäynnin kannalta keskeisiä antennin ominaisuuksia ovat myös antennikeilan *muoto* ja *keilanleveys* sekä *antennivahvistus*, jotka liittyvät toisiinsa. Antenni ei säteile tai vastaanota signaaliaan tasaisesti joka suuntaan, vaan se rakennetaan suuntaamaan tehoa tiettyyn suuntaan. Antennin keilaa voidaan muotoilla: esimerkiksi ilmavalvontatutkissa tarvitaan yleensä korkea keila, jotta havaitaan kaikilla korkeuksilla lentävät maalit. Asejärjestelmien maalinseuranta-tutkissa antennikeila puolestaan on kapea sekä vaaka- että pystysuunnissa, jotta maalin sijainti voidaan määrittää mahdollisimman tarkasti asejärjestelmän ohjausta varten.

Antennin keilanleveys kuvaa keilan kokoa kulmayksiköissä, asteina tai radiaaneina. Mikäli antenni olisi ympyräsäteilevä eli säteilisi tehoaan tasaisesti joka suuntaan, olisi sen vahvistus 1 = 0 dB, koska tehoa ei synny antennissa mistään lisää. Antennin kapeasta keilasta on kuitenkin hyötyä: kun lähettimestä tulevaa signaalitehoa ei lähetetäkään kaikkiin mahdollisiin suuntiin, vaan vain kapeaan keilaan, kyseiseen suuntaan lähetetty tehotiheys kasvaa huomattavasti. Näin antennikeilaa kaventamalla voidaan haluttuun suuntaan lähettää huomattavasti suurempi signaaliteho kuin leveällä keilalla, ja vastaavasti kapealla keilalla voidaan havainnoida huomattavasti heikompia signaaleja. Järjestelmän ulottuvuus siis kasvaa.



**Kuva L5.1: Vahvistavalla antennilla voidaan lähettää enemmän säteilytehoa tiettyyn suuntaan ympärisäteilevään antenniin verrattuna, ja vastaanottaa voimakkaammin kyseisestä suunnasta tulevia signaaleja. Tätä havainnollistaa polttimo ja heijastin (vrt. paraboloidiantenni): Ilman heijastinta lamppu valaisee lähes joka suuntaan. Tällöin voidaan nähdä eri suunnissa olevia kohteita, kunhan ne eivät vain ole liian kaukana. Heijastin kohdistaa valokeilan yhteen suuntaan, jolloin keilan valaisemat kohteet havaitaan paremmin ja kauempaa. Tällöin kokonaiskuva kuitenkin kärsii, koska kapean keilan valaiseman alueen ympärillä olevia muita kohteita ei havaita.**

Antennivahvistukset vaihtelevat käytännössä dipoliantennin noin 2 dB:n vahvistuksesta paraboloidiantennien useiden kymmenien desibelien (20..35 dB) vahvistukseen. On syytä huomata antennin keilakuvioon/keilanleveyteen ja vahvistukseen liittyvä kaksijakoinen optimointiongelma:

1. Kapea antennikeila parantaa järjestelmän toimintaetäisyyttä hyvän antennivahvistuksen myötä. Kapea antennikeila mahdollistaa myös haitallisten signaalien sulkemisen kulloinkin tarkasteltavan alueen ulkopuolelle.

2. Kapea antennikeila rajaa kerrallaan tarkasteltavan alueen pieneksi. Tällöin kokonaistilanteen hahmottaminen edellyttää antennin kääntelemistä eri suuntiin. Ympärisäteilevät antennit ovat tämän vuoksi tärkeitä useissa taktisissa tiedustelujärjestelmissä, joiden tehtävänä on esimerkiksi antaa nopeasti uhkavaroitus.

*Antennin pääkeila* kuvaa suuntaa, johon suurin osa antennin säteilystä suuntautuu. Säteilyä vuotaa kuitenkin myös muihin suuntiin. Vastaavasti antenni myös vastaanottaa signaaleja näistä suunnista, joita kutsutaan *sivu-* ja *takakeiloiksi*. Taka- ja sivukeilojen voimakkuus ilmaistaan yleensä suhteessa pääkeilan voimakkuuteen. Esimerkiksi jos antennin vahvistus (siis pääkeila) on 30 dB ja antennin sivukeilataso on 13 dB, on antennin vahvistus sivukeilan suuntaan 30 dB - 13 dB = 17 dB, mikä on sekin huomattava antennivahvistus ja voi aiheuttaa ongelmia. Sivukeilojen minimointi onkin eräs keskeisiä antennisuunnittelun päämääriä ja keinoja suojautua elektroniselta häirinnältä ja tiedustelulta. Sivukeilataso ilmoitetaan taulukoissa usein suhteessa pääkeilaan, mikä vuoksi sivukeilataso ilmoitetaan taulukoissa usein negatiivisena.

Seuraavat kaksi antenneihin liittyvää riippuvuutta on tärkeää ymmärtää järjestelmien elektronisen suojautumisen suorituskykyä arvioitaessa. Apertuuriantennin (esim. paraboloidipeiliantennin) keilanleveys riippuu suoraan signaalin aallonpituudesta ja kääntäen antennin halkaisijasta seuraavan kaavan mukaan:

$$\Theta \approx 60° \cdot \frac{l}{D}$$

missä $\Theta$ on keilanleveys asteina halkaisijaa vastaavassa suunnassa, $l$ aallonpituus ja $D$ antennin halkaisija.[nn] Ympyrän muotoisella antennilla keilanleveys on vakio kaikissa suunnissa, mutta esimerkiksi ilmavalvontatutkissa on tyypillisesti soikion muotoinen antenni, jolla keilanleveydet vaaka- ja pystysuunnassa ovat erilaiset ja kumpikin erikseen arvioitavissa em. kaavalla. Kuvassa L5.2 esitetään antennikeilan keskeisten piirteiden nimitykset. Pääkeilan osalta on pidettävä mielessä, että sen leveys määritellään yleensä 3 dB tason mukaan. Pääkeilan reunoilla signaalin tehotaso on siis 3 dB eli puolet pienempi kuin maksimikohdassa.

Kun antennin keilanleveydet vaaka- ja pystysuunnassa tunnetaan, voidaan arvioida antennin vahvistus *desibeleinä* seuraavan kaavan mukaisesti:

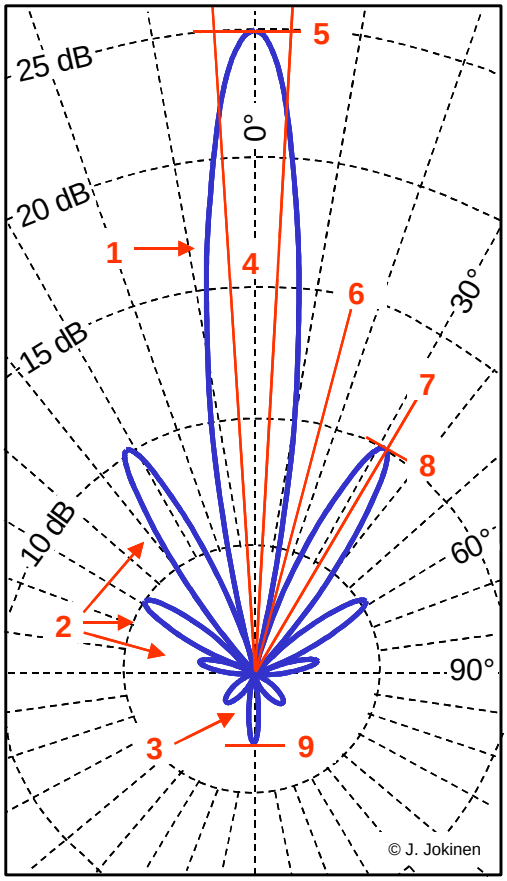
$$G \approx 44 - 10 \cdot \log_{10}(\Theta_V \cdot \Theta_P)$$

missä $G$ on antennivahvistus desibeleinä, $\Theta_V$ ja $\Theta_P$ antennin keilanleveydet asteina vaaka- ja pystysuunnassa[oo]. Esitettyjen kaavojen perusteella voidaan esimerkiksi suorittaa nopeasti seuraava päättelyketju:

> Jos hävittäjätutkan taajuus on 10 GHz, on sen aallonpituus 30 cm/10 = 3 cm. Jos tutkan pyöreän antennin halkaisija on 1 m, on antennin keilanleveys pysty- ja vaakasuunnassa 60° x 3 cm / 100 cm = 1,8°. Antennin vahvistus desibeleinä on suuruusluokaltaan 44 - 10 x $\log_{10}$(1,8 x 1,8) = 39 dB.

[nn] Antennin muista ominaisuuksista riippuen kerroin 60 voi vaihdella todellisuudessa noin välillä 50-70, mutta esitetty kaava antaa riittävän hyvän karkean suorituskykyarvion.

[oo] Kaavaa varten antennista on tehty tiettyjä oletuksia, mutta tarkkuus riittää karkeaan suorituskykyarvioon.




**Kuva L5.2: Esimerkki antennin keilakuviosta planaaritasossa.**

1. **pääkeila**
2. **sivukeilat**
3. **takakeila**
4. **pääkeilan keilanleveys (8°)**
5. **pääkeilan voimakkuus (25 dB)**
6. **ensimmäisen säteilyminimin (16°)**
7. **ensimmäisen sivukeilan suunta (32°)**
8. **ensimmäisen sivukeilan voimakkuus (-15 dB suhteessa pääkeilaan = 10 dB)**
9. **takakeilan voimakkuus (-19 dB suhteessa pääkeilaan = 6 dB)**

## Vastaanotin – tasapainoilua eri vaatimusten ja luonnonlakien välillä

ELSO-järjestelmässä vastaanottimelle on asetettu lukuisia vaatimuksia: vastaanottimen *taajuusalueen* tulee olla uhkaympäristöön sopiva ja sen (taajuus)*kaistanleveyden* tulee olla mahdollisimman suuri. ELSO-vastaanottimella tulee olla hyvä *taajuudenmittauskyky* ja *taajuuserottelukyky* sekä hyvä *herkkyys*. Vastaanottimen herkkyydellä tarkoitetaan heikointa mahdollista ilmaistavaa signaalia. Koska signaali vaimenee edetessään, herkkyys vaikuttaa suoraan ELSO-järjestelmien ja vastaanottimia hyödyntävien ELSO:n kohdejärjestelmien ulottuvuuteen. Järjestelmän herkkyys riippuu vastaanottimen ja järjestelmän muiden elektronisten komponenttien kohinatasosta. Järjestelmässä syntyvä terminen kohina eli satunnainen haitallinen häiriösignaali, jota ei saa suodatettua hyötysignaalista pois, on luonnonlaeista seuraava reunaehto jokaiselle elektroniselle komponentille. Terminen kohina on luonnon asettama raja, johon todellisissa elektronisissa järjestelmissä ei koskaan päästä. Järjestelmien kohinaominaisuuksia kuvataan usein *kohinaluvulla*, joka kertoo kuinka monta desibeliä huonompi järjestelmän kohinataso on ideaaliseen verrattuna. Täsmälleen kohinatason suuruista signaalia ei kuitenkaan käytännössä havaita kohinan

seasta, vaan tarvitaan lisäksi tietty *prosessoinnin kynnystaso*, jonka ylittävä signaali tulkitaan todelliseksi signaaliksi eikä kohinapiikiksi. Vastaanotinmittauksissa usein käytettävä ns. tangentiaalinen herkkyys vastaa noin 8 dB:n ylitystä kohinatasoon. Automaattiset ELTU-järjestelmät voivat vaatia jopa 15 dB kohinaa voimakkaampaa signaalia.

Ideaalisesta pohjakohinasta, kohinaluvusta ja prosessointikynnyksestä saadaan laskettua kokonaisen vastaanotinjärjestelmän herkkyys kaavalla (desibeliyksiköissä):

$$S_{MIN} = -114\,\mathrm{dBm} + 10 \cdot \log_{10}(B_{MHz}) + F + M$$

missä $S_{MIN}$ on kokonaisjärjestelmän herkkyys, $B_{MHz}$ kaistanleveys mega-hertseinä, $F$ järjestelmän kohinaluku ja $M$ prosessoinnin kynnystaso. Tässä ei kuitenkaan ole koko totuus: lisäämällä järjestelmään voimakkaasti vahvistava antenni voidaan herkkyyttä parantaa antennivahvistuksen verran. Kokonaisjärjestelmän herkkyystasoa, johon on huomioitu antennivahvistus, kutsutaan *isotrooppiseksi herkkyydeksi*. Isotrooppinen herkkyys saadaan vähentämällä vastaanottimen herkkyydestä antennivahvistuksen arvo.

Mikroaaltoalueella realistisia arvoja voisivat olla seuraavat: kaistanleveys 500 MHz, kohinaluku 13 dB ja prosessoinnin kynnystaso 8 dB tuottavat herkkyydeksi -66 dBm. Käyttämällä järjestelmässä 34 dB:n peiliantennia isotrooppiseksi herkkyydeksi saadaan -100 dBm. Tämä kuvaa signaalivoimakkuutta, jonka järjestelmä kykenee havaitsemaan antennin pääkeilan suunnasta.

Edellä olevasta kaavasta voidaan havaita myös vastaanottimen taajuuskaistan vaikutus herkkyyteen: mitä leveämpi kaista, sitä huonompi herkkyys! Koska herkkyys vaikuttaa järjestelmän ulottuvuuteen, saadaan herkällä järjestelmällä havaittua heikkoja signaaleja, siis kauempana sijaitsevia lähettimiä. Tämä on jälleen kaksijakoinen optimointiongelma: kaistanleveyden pienentäminen parantaa kantamaa, mutta heikentää kokonaiskuvaa. Laajalla kaistanleveydellä saadaan seurattua useaa eri lähetettä yhtä aikaa, tai esim. seurattua taajuushyppivää lähetettä, kun taas kapea taajuuskaista edellyttää vastaanottimen kulloinkin tarkasteleman taajuuskaistan siirtelyä, jolloin puhutaan pyyhkäisevästä vastaanottimesta.

## Signaalien tehobudjetti – yksisuuntaisen yhteyden neliölaki

Edetessään lähettimen antennista vastaanottoantenniin radioaalto vaimenee *neliöllisesti* (eli suhteessa etäisyyden toiseen potenssiin). Tämä tarkoittaa sitä, että etäisyyden kaksinkertaistuessa signaaliteho pienenee neljänteen osaan, kolminkertaistuessa yhdeksänteen osaan jne. Tämä johtuu avaruuden kolmiulotteisuudesta ja vertautuu esim. ilmapallon puhaltamiseen: kumia (signaalienergiaa) on tietty kokonaismäärä pallossa (esim. tutkapulssissa), ja pallon (aaltorintaman) edetessä kumia

(signaalitehotiheyttä) on aina ohuempi kerros eli pienempi määrä tiettyä pinta-alaa kohti. Ilmiötä kuvattaessa puhutaankin radioaaltojen pallolaajenemisesta.

Yksisuuntainen neliöllisen lain mukainen signaalin vaimeneminen toteutuu esim. radioyhteyksissä, ja elektronisen sodankäynnin viitekehyksessä tiedusteltavan signaalin etenemisessä kohdejärjestelmästä tiedustelujärjestelmän antenniin, sekä häirintä-signaalin etenemisessä häirintälähettimestä häirittävään kohdejärjestelmään.

Signaalin vaimenemisen kaavoihin ei ole syytä mennä tarkemmin, mutta asiaan vaikuttavien tekijöiden ymmärtämiseksi seuraavassa yhteysvälin maksimietäisyyden vapaassa tilassa määräävä kaava (lineaarisissa yksiköissä):

$$R_{MAX} = \frac{l}{4p}\sqrt{\frac{P_L G_L G_V}{S_{MIN} L}}$$

missä $R_{MAX}$ on yhteyden maksimietäisyys, $l$ aallonpituus, $P_L$ lähetysteho, $G_L$ lähetysantennin vahvistus, $G_V$ vastaanottoantennin vahvistus, $S_{MIN}$ vastaanottimen herkkyys (pienin havaittavissa oleva signaaliteho) ja $L$ sekalaiset vaimenemistekijät (ilmakehä, sääilmiöt yms.). Kaavan neliöllisyys tarkoittaa, että signaalitehon tai jommankumman antennivahvistuksen nelinkertaistaminen ainoastaan kaksinkertaistaa yhteysetäisyyden eli lisätehoa tai -vahvistusta tarvitaan hyvin paljon yhteysvälin oleelliseen lisäämiseen.[pp] Samoin herkkyyden nelinkertainen paraneminen (pieneneminen) ainoastaan kaksinkertaistaa kantaman.

Usein puhutaan ns. EIRP-tehosta (Equivalent Isotropic Radiated Power), joka tarkoittaa lähetystehon ja lähetysantennin vahvistuksen tuloa $EIRP = P_L$ x $G_L$ (tai desibeleinä summaa $EIRP_{dB} = P_L + G_L$). Termi kuvaa, miten tehokkaasti kokonais-järjestelmä säteilee signaalitehoa tiettyyn (esim. pääkeilan) suuntaan. Nimenomaan tämä lähettimen ja antennin yhteisvaikutus kuvaa järjestelmän suorituskykyä[qq].

Vapaan tilan vaimennus edellyttää esteetöntä yhteysväliä, joten se rajautuu radio-horisonttiin. Radiohorisontti on hiukan optista horisonttia kauempana ja se lasketaan yleensä kaavalla[rr]:

$$R = 4{,}1 \cdot \sqrt{h_1} + 4{,}1 \cdot \sqrt{h_2}$$

---

[pp] Desibelejä käytettäessä signaalitehon tai antennivahvistuksen kaksinkertaistaminen tarkoittaa 3 dB:n lisäystä, nelinkertaistaminen 6 dB:n lisäystä.

[qq] EIRP-tehon tilalla puhutaan yleisesti samassa merkityksessä myös ERP-tehosta (Effective Radiated Power). Täsmällisen määritelmän mukaan ERP on kuitenkin normitettu dipoliantennille, kun taas EIRP-tehoa verrataan ympärisäteilevään antenniin, kuten ELSO-laskuissa yleensä muuten oletetaan. ERP-arvo on siten n. 2 dB pienempi kuin vastaava EIRP-arvo, ja EIRP on ELSO-yhteyksissä yleensä täsmällisempi termi.

[rr] Radiohorisonttia käsitellään tarkemmin liitteessä 2, missä sille on taulukoitu esimerkkiarvoja.

missä $R$ on radiohorisontti kilometreinä, $h_1$ lähetysantennin korkeus metreinä ja $h_2$ vastaanottoantennin (tai esim. tutkan maalin) korkeus metreinä. Esimerkiksi antennikorkeuksilla 20 m radiohorisontti on noin 37 km, jota pidemmillä yhteyksillä signaali siis vaimenee erittäin voimakkaasti.

Vapaa tila ei toteudu myöskään metsässä, taajamassa tai muissa tyypillisissä maasto-olosuhteissa. Näiden tilanteiden yhteysvälivaimenemisen matemaattista käsittelyä varten on kehitelty erilaisia vaimennusmalleja, kuten Egli, Murphy, Hata jne. Ne on mitattu tietyissä olosuhteissa tietyille taajuuksille, ja niiden tarkkuus on usein hyvin vaatimaton.

Vaimenemista arvioitaessa on muistettava, että eri taajuusalueilla on omat erityis-ominaisuutensa, kuten HF-taajuuksien heijastuminen ionosfääristä ja siten eteneminen jopa maapallon toiselle puolelle. Sääilmiötkin voivat aiheuttaa omat seurauksensa: tietyissä olosuhteissa radioaalto voi kanavoitua merenpinnan yläpuolella ja edetä huomattavasti oletettua pidemmälle.

## Signaalien tehobudjetti – tutkan neljännen potenssin laki

Yksisuuntainen yhteys vaimenee neliöllisesti, mutta tutkan signaali vaimenee ensin neliöllisesti edetessään tutkasta maaliin, heijastuu tai siroaa[ss] maalista vain osittain takaisin kohti tutkaa ja vaimenee jälleen neliöllisesti edetessään takaisin kohti tutkan antennia. Kaksisuuntaisen etenemisen vuoksi tutkasignaali vaimenee etäisyyden neljänteen potenssiin verrannollisesti eli oleellisesti enemmän kuin yksisuuntaisen yhteyden signaalit. Etäisyyden kaksinkertaistuessa signaalivoimakkuus pienenee kuudenteentoista osaan, kolminkertaistuessa 81. osaan jne. Tutkan maksimi-mittausetäisyyden kaava vapaassa tilassa (lineaarisissa yksiköissä) on:

$$R_{MAX} = \sqrt[4]{\frac{P_L G^2 l^2 s}{(4p)^3 S_{MIN} L^2}}$$

missä $R_{MAX}$ on tutkan maksimimittausetäisyys, $P_L$ lähetysteho, $G$ tutkan antennin vahvistus, $l$ aallonpituus, $s$ maalin tutkapoikkipinta (maalin kokoa ja muotoa kuvaava suure), $S_{MIN}$ tutkan vastaanottimen herkkyys (pienin havaittavissa oleva signaaliteho) ja $L$ sekalaiset vaimenemistekijät (ilmakehä, sääilmiöt yms.)[tt].

Tutkan mittausetäisyyden kaava on siten hyvin samankaltainen kuin yksisuuntaisen yhteyden kaava, mutta neljännen potenssin (tai neljännen juuren) riippuvuus tekee

[ss] Tutkapulssi heijastuu maalin metallipinnoista kuin valo peilistä, mutta osuessaan kohteeseen, jonka koko on aallonpituuden suuruusluokkaa, tutkapulssi siroaa lukuisiin eri suuntiin.

[tt] Kaava on muodostettu tutkan yhdelle pulssille. Tutkan etuna voi kuitenkin olla ns. *koherentti integrointi*, missä tutka lähettää useita pulsseja ja prosessoi ne yhdessä, parantaen herkkyyttä ja siten saaden hiukan lisää kantamaa. Häviötermiksi $L$ esitetään tässä yhdensuuntaiset häviöt; koska signaali etenee ensin maaliin ja sitten takaisin, kokonaishäviöt ovat $L^2$.

hyvin dramaattisen vaikutuksen mittausetäisyyteen ja vastaanotettuun signaali-voimakkuuteen etäisyyden kasvaessa. Tutkan lähetystehon pitäisi siis kuusitoista-kertaistua, jotta tutkan kantama kaksinkertaistuisi. On myös syytä huomata maalin tutkapoikkipinnan rooli: nimenomaan tätä tekijää pyritään pienentämään rakennet-taessa häivelentokoneita ja -aluksia (stealth). Kohteita pyritään pinnoittamaan tutkasäteilyä absorboivilla pinnoitteilla, jotka estävät tutkasignaalin säteilyn takaisin maalista, tai kohteet muotoillaan siten, että tutkasäteily heijastuu muualle kuin takaisin tutkan suuntaan.

## Häirinnän ja hyötysignaalin taistelu

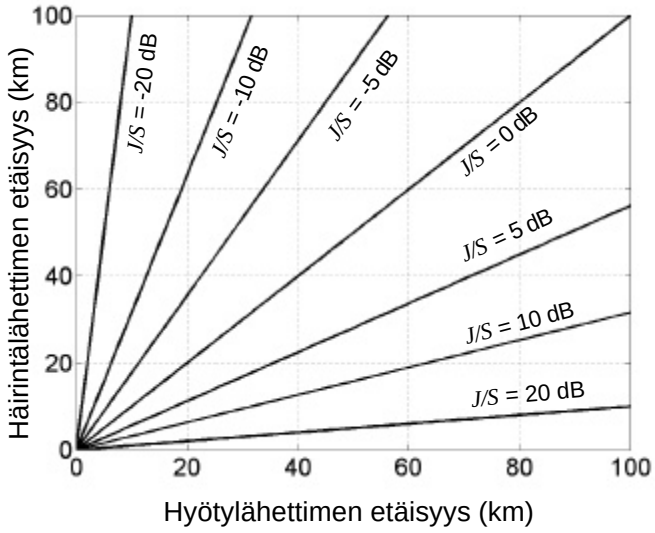
Elektronisessa häirinnässä häirittävän kohteen vastaanottimeen pyritään tyypillisesti saamaan vastaanotettua hyötylähetettä voimakkaampi häirintäsignaali. Tällöin häirintäsignaali peittää hyötysignaalin, jolloin esimerkiksi tutka ei kykene tulkitsemaan onko sen vastaanottamassa signaalissa todellinen maalikaiku vaiko ei, jolloin häirintä onnistuu. Matemaattisissa häirintäanalyyseissa lasketaan yleensä *häirintä-signaalisuhteita* (*J/S;* Jamming/Signal), jotka kuvaavat miten paljon häirintäsignaali on hyötysignaalia voimakkaampi tai heikompi. Esim. *J/S* = 20 dB tarkoittaa, että häirintäteho on tutkavastaanottimessa satakertainen hyötysignaalin tehoon verrattuna.

Aiemmin käsiteltyjä signaalin tehobudjettikaavoja ja muita vastaavia yhtälöitä voidaan käyttää tarkasteltaessa häirintä- ja hyötysignaalitehojen suhteita. Esim. viestiliikenne-yhteyttä häirittäessä sekä häirintä- että hyötysignaali vaimenevat neliöllisesti, ja häirintä-signaalisuhde saa seuraavan kaavan muodon (hiukan yksinkertaistettuna, lineaarisissa yksiköissä):

$$J/S = \frac{P_{LJ} G_{LJ} G_{VJ}}{P_{LS} G_{LS} G_{VS}} \cdot \left( \frac{R_S}{R_J} \right)^2$$

missä $P_{LJ}$ häirintälähettimen lähetysteho ja $P_{LS}$ on hyötysignaalin lähetysteho; $G_{LJ}$ on häirintäjärjestelmän antennivahvistus ja $G_{LS}$ hyötysignaalilähettimen antennivahvistus häirittävän järjestelmän suuntaan. $R_S$ on hyötylähettimen etäisyys häiritystä järjestelmästä ja $R_J$ häirintäsignaalin etäisyys häiritystä järjestelmästä. Häirittävän järjestelmän antennivahvistuksessa tulee huomioida, että jos häirintälähetin on eri suunnassa kuin hyötylähetin, antennivahvistukset eivät ole samat. Häirityn kannalta ideaalitilanteessa hyötysignaali on antennin pääkeilassa ja häirintäsignaali tulee hyvin heikkona sivukeilan kautta. Vastaavasti häiritsijä pyrkii saamaan häirintäsignaalinsa sisään antennin pääkeilasta tai mahdollisimman vahvasta sivukeilasta. Kaavassa näitä antennivahvistuksia ovat häirittävän järjestelmän antennivahvistus häirintäsignaalin suuntaan $G_{VJ}$ ja häirittävän järjestelmän antennivahvistus hyötysignaalin suuntaan $G_{VS}$. Kuvasta L5.3 nähdään häirintä-signaalisuhteen riippuvuus hyöty- ja häirintälähettimien etäisyyksistä vapaan tilan etenemisen tilanteessa. Todellisissa maassa toimivien järjestelmien tapauksissa tilanne ei ole näin suoraviivainen, vaan vapaata tilaa monimutkaisempi yhteysvälivaimennus, signaalin monitie-eteneminen ja muut todelliseen signaaliympäristöön liittyvät tekijät

tekevät tilanteen oleellisesti monimutkaisemmaksi[uu]. Tilanteeseen vaikuttaa luonnollisesti myös em. kaavan muut tekijät, mutta kuvassa nämä on oletettu kaikki vakioiksi – todellisessa tilanteessa ne nostavat tai laskevat suhdetta huomattavasti suuntaan tai toiseen, erityisesti häirinnän kohteen antennivahvistukset eri suuntiin ovat kriittisiä ja voivat muuttaa tilannetta kymmeniä desibelejä suuntaan tai toiseen.




**Kuva L5.3: Häirintä-signaalisuhteen riippuvuus hyöty- ja häirintälähettimien etäisyyksistä vapaan tilan yhteysvälivaimenemisen tilanteessa. Lähetystehot ja antennivahvistukset on oletettu samoiksi kummallekin lähettimelle. Valitse vaaka- ja pystyakseleilta etäisyydet; niiden risteämiskohta ilmaisee häirintä-signaali-suhteen.**

Kuvasta tulee erityisesti huomata häirintälähettimen suhteellisen etäisyyden vaikutus häirintätilanteeseen: esim. kun hyötylähetin on 25 km:n etäisyydellä ja häirintälähetin 80 km:n etäisyydellä, on häirintä-signaalisuhde noin -10 dB eli häirintäsignaali on teholtaan kymmenesosa hyötysignaalista ja hyötylähete päässee helposti läpi. Häirintä-lähettimen on tultava muutaman kilometrin etäisyydelle nostaakseen häirintä-signaali-suhteen 20 dB:n arvoon, jolloin tilanne heikkenee häirittävän kannalta 30 dB. Tämän vuoksi lähihäirintälähettimet voivat olla hyvinkin tehokkaita, vaikka niiden häirintäteho olisikin vaatimaton.

Edellä käsitelty koskee esim. viestisignaalin tai tiedusteluvastaanottimen häirintää, mutta tilanne muuttuu häiritsijän kannalta oleellisesti paremmaksi tutkia häirittäessä. Koska häirintäsignaali heikkenee suhteessa etäisyyden toiseen potenssiin, mutta

[uu] Esimerkiksi tutkassa signaalin heijastuminen maanpinnasta johtaa siihen, että antennin vertikaalinen suuntakuvio liuskoittuu. Tällöin siihen muodostuu maksimi- ja minimikohtia. Kantaman kannalta tämä merkitsee sitä, että maalin korkeudesta riippuen tutkan kantama on ao. kokoiseen maaliin joko nolla tai vastaavasti kaksinkertainen normaalitilanteeseen verrattuna.

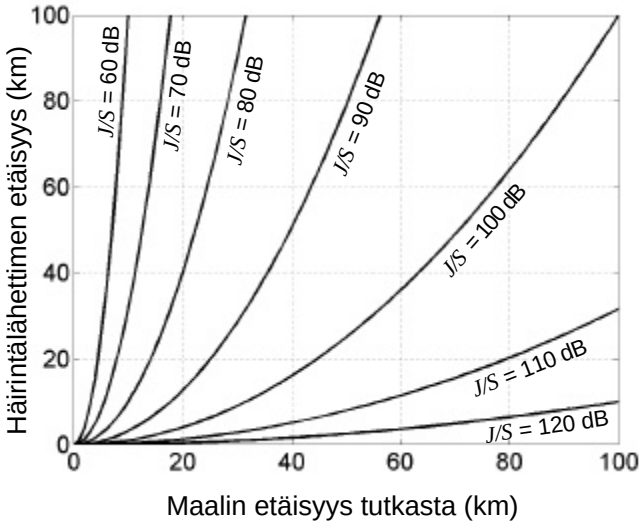
tutkamaalin kaikusignaali aiemmin kuvatun mukaisesti suhteessa neljänteen potenssiin, on häiritsijä vahvoilla pitkähköillä tutkamittausetäisyyksillä.

Tutkan tapauksessa, hiukan yksinkertaistettuna ja lineaarisissa yksiköissä ilmaistuna, tutkan häirintä-signaalisuhteeksi saadaan:

$$J/S = \frac{P_{LJ} G_{LJ} G_{VJ}}{P_{LS} G^2} \cdot \frac{R_S^4}{R_J^2} \cdot \frac{4p}{s}$$

missä termit ovat kuten edellisessä kaavassa. *G* on tutka-antennin antennivahvistus maalin (pääkeilan) suuntaan, ja *s* on tutkamaalin tutkapoikkipinta.

Etäisyyksiin vaikuttavien potenssien lisäksi kaavasta voidaan myös huomata miten (omasuoja)häirintää voidaan tehostaa pienentämällä lavetin (tutkamaalin) tutkapoikkipintaa.



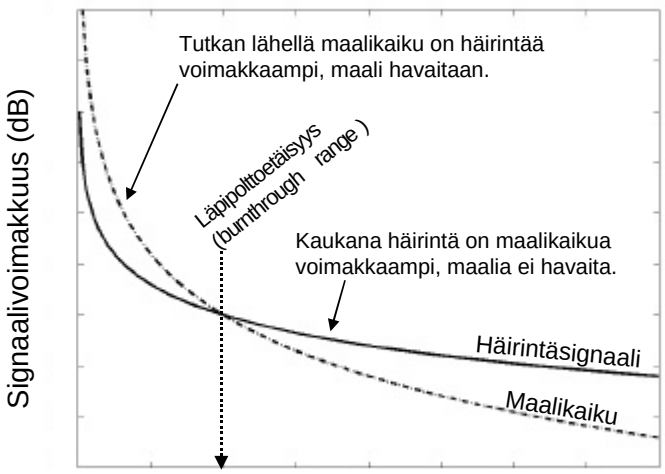

**Kuva L5.4: Tutkan häirintä-signaalisuhteen riippuvuus maalin ja häirintälähettimen etäisyyksistä vapaan tilan yhteysvälivaimenemisen tilanteessa isohkolle lentokonemaalille. Lähetystehot ja antennivahvistukset on oletettu samoiksi kummallekin lähettimelle – mikä on tietenkin täysin epärealistinen tilanne (vähennä arvoista lähetystehojen ja antennivahvistusten erot), mutta kuva antaa mielikuvaa tilanteen hankaluudesta tutkan kannalta verrattuna viestijärjestelmään kuvassa L5.3.**

Kuvassa L5.4 on edellistä kuvaa vastaavasti esitetty häirintä-signaalisuhteen riippuvuus tutkamaalin ja häirintälähettimien etäisyyksistä vapaan tilan etenemisen tilanteessa. Lähetystehot ja antennivahvistukset on todellisesta tilanteesta poiketen oletettu samoiksi häiritsijälle ja tutkalle, ja kaavaa muutenkin yksinkertaistettu hiukan – kuva on tehty ainoastaan antamaan mielikuvaa tilanteesta.

Kuvasta nähdään, että tutkaa häirittäessä tilanne on olennaisesti toinen kuin yksisuuntaista yhteyttä häirittäessä. Häiritsijällä on huomattava etulyöntiasema tutkan mittausetäisyyden kasvaessa. Vaikka häiritsijä toimisikin sivukeilasta, voi kuvan osoittama kymmenien desibelien häirinnän etulyöntiasema kuitenkin taata häirinnän onnistumisen.

Erityistilanteena voidaan tarkastella tutkan omasuoja- tai saattohäirintää, missä maalin etäisyys ($R$) on sama kuin häirintäetäisyys ja häirintä pääsee järjestelmään sisään tutkan pääkeilasta ($G_{VJ}=G$). Tällöin häirintä-signaalisuhde yksinkertaistuu muotoon:

$$J/S = \frac{P_{LJ}G_{LJ}}{P_{LS}G} \cdot R_S^2 \cdot \frac{4p}{s}$$




**Kuva L5.5: Tutkan maalikaiun ja häirintäsignaalin voimakkuudet eri etäisyyksillä tutkasta omasuojahäirinnän ja vapaan tilan vaimenemisen tapauksessa. Tarpeeksi lähellä tutkaa häirintäsignaali ja maalikaiku ovat yhtä suuret, maali on ns. läpipolttoetäisyydellä ja se havaitaan tutkalla. Mikäli kuitenkin häirintätehoa kasvatetaan (käyrä nousee kuvassa ylöspäin) tai häivetekniikka pienentää maalikaiun voimakkuutta (käyrä laskee kuvassa alaspäin), läpipolttoetäisyys siirtyy lähemmäksi tutkaa.**

Kuvassa L5.5 on esitetty tutkahäirinnän potenssilakien keskeisin sisältö konkretisoituna omasuojahäirinnän tilanteeseen: lavetin ollessa kaukana tutkasta häirintäsignaali saadaan helposti paljon voimakkaammaksi kuin maalin kaikusignaali eli häirintä on tehokasta ja maalia ei havaita. Tietyllä etäisyydellä maalikaiun voimakkuus kuitenkin nousee samalle tasolle kuin häirintäsignaali. Tätä etäisyyttä kutsutaan *läpipolttoetäisyydeksi* (burnthrough range). Tätä lähempänä maalikaiku on häirintää voimakkaampi, ja maali havaitaan tutkalla. Lavetin häivetekniset ratkaisut tai häirintäjärjestelmän tehon lisääminen voivat kuitenkin parantaa tilanteen siten, että

läpipolttoetäisyys pienenee huomattavasti, ja ehkä niin pieneksi, että aselavettien väliin jää turvallinen käytävä.

## Infrapunasäteilyn ominaisuuksia – jokainen säteilee, haluaa tai ei

Suuri osa elektronisen sodankäynnin ongelmakentästä keskittyy radiotaajuiselle sähkömagneettisen spektrin alueelle, mutta myös optinen spektrin alue on tärkeä osa elektronista taistelua ja erityisesti sen infrapuna-alue on keskeinen sodankäynnissä.

Infrapuna-alueella voidaan toimia kuten RF-alueen tutkasovelluksissa esimerkiksi lähettämällä aktiivisesti infrapunasignaalia ja mittaamalla kohteesta saatu heijastus (esim. IP-laseretäisyysmittarit ja -tutkat), tai kuten viestisovelluksissa esim. käyttämällä IP-lasereita aktiivisesti tietoliikenteeseen. Sodankäynnissä keskeisessä roolissa on kuitenkin ns. terminen infrapunasäteily (lämpösäteily), jota ei tuoteta tarkoituksella keinotekoisesti, vaan jota kaikki kappaleet säteilevät ympäristöönsä. Termisen IP-säteilyn voimakkuus eri aallonpituusalueilla riippuu kohteen lämpötilasta, sen pinnan ominaisuuksista ja ilmakehän läpäisystä. Kohteen lämpötilaa ja pinnan säteilyominaisuuksia voidaan muokata, mutta vanhan totuuden mukaan lämmöstä ei päästä eroon – sitä voidaan vain siirtää eri paikkoihin.

Kuvasta L5.6 nähdään ns. Planckin lain mukainen mustan kappaleen säteily. Ideaalinen ”musta” kappale säteilee infrapunasäteilyä tämän lain mukaan. Todelliset kappaleet eivät säteile aivan teoreettisen voimakkaasti: niiden säteilyhyötysuhdetta kuvaa ns. emissiivisyyskerroin, joka on todellisen säteilytehon suhde Planckin lakiin. Se on useilla tavanomaisilla materiaaleilla yli 80%, mutta esim. kiillotetuilla metallipinnoilla vain muutamia prosentteja. Todellisen materiaalin emissiivisyys riippuu myös aallonpituudesta.

Infrapunataajuusalueella häivetekniikka (stealth) perustuu siihen, että kappaleen tuottama heräte (säteilytehotiheys kullakin taajuudella) pyritään muokkaamaan ympäristöä vastaavaksi. Maastossa oleva ihminen on lähes saman lämpöinen kuin kesäinen metsä, mutta mikäli ihmisen vaatteiden emissiivisyys tietyllä infrapuna-alueella poikkeaa huomattavasti taustan emissiivisyydestä, voidaan ihminen havaita lämpökameralla ympäristöä voimakkaamman tai heikomman säteilyn vuoksi. Toisaalta ympäristöä kuumemmat kappaleet säteilevät enemmän kuin ympäristö – tällöin häiveratkaisussa lämpö pyritään pitämään poissa kappaleen pinnasta esim. laittamalla ajoneuvon ympärille ilmaraon päähän naamioverkko tai jäähdyttämällä pintaa, tai vaihtoehtoisesti voidaan yrittää muokata pinnan emissiivisyyttä.

Kuvasta L5.6 nähdään myös eri infrapuna-aallonpituusalueet[vv]. Alle 780 nm:n säteily on jo näkyvää valoa, minkä seurauksena kuvan mukaisesti aurinko ja muut tuhansien

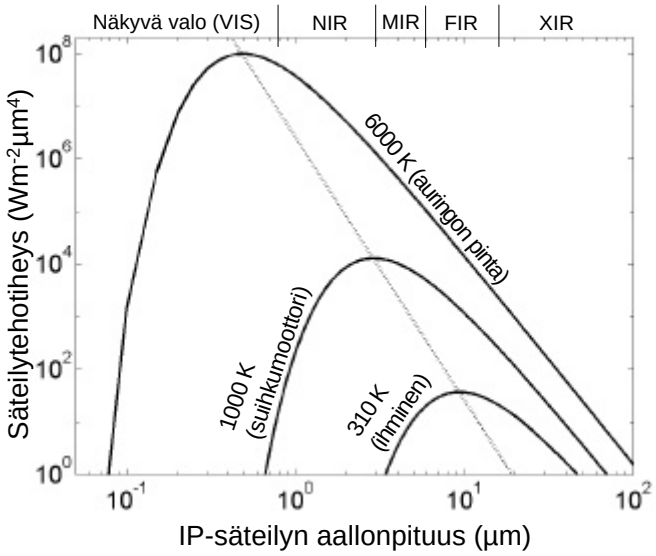
[vv] VIS = näkyvän valon alue, NIR = lähi-infrapuna, MIR = keski-infrapuna, FIR = kaukoinfrapuna, XIR = ääri-infrapuna

asteiden lämpöiset kappaleet säteilevät runsaasti näkyvää valoa. Esim. lentokoneen suihkumoottorin sisälämpötilan aiheuttama lämpösäteily osuu pitkälti lähi-infrapuna-alueelle (NIR; 0,78-3 µm), minkä vuoksi takaa avonaisina näkyviin suihkumoottoreihin hakeutuvat infrapunaohjusten hakupäät toimivat usein tällä aallonpituusalueella. Ihmisen, ajoneuvojen ja useimpien luonnon kohteiden infrapunasäteily osuu suurelta osin kaukoinfrapuna-alueelle (FIR; 6-15 µm), minkä vuoksi lämpökamerat toimivat yleensä tällä alueella.

Kuvasta L5.6 havaittiin, että kappaleen lämmön kasvaessa sen säteilemän infrapunasäteilyn tehotiheysmaksimi siirtyy kohti pienempiä aallonpituuksia (kuvan katkoviiva). Tätä riippuvuutta kuvaa ns. Wienin siirtymälaki, jonka avulla voidaan laskea mille infrapuna-aallonpituusalueelle tietyn lämpöisen kappaleen infrapuna-säteilyn maksimi osuu:

$$l_{MAX} = \frac{2898\,\mu\mathrm{m}}{T}$$

missä $l_{MAX}$ on infrapunasäteilyn tehotiheysmaksimin aallonpituus ja $T$ kappaleen lämpötila. Näin ollen esim. 1000 K:n lämpöisen suihkumoottorin säteily-maksimi on 2,9 µm:n kohdalla lähi-infrapuna-alueella, ihmisen (37°C=310 K) 9,3 µm:n kohdalla kaukoinfrapuna-alueella.




**Kuva L5.6: Mustan kappaleen säteily Planckin lain mukaan eri lämpöisille kappaleille.**

Kuva L5.6 osoittaa myös, että kappaleen lämpötilalla on hyvin voimakas vaikutus kappaleen säteilytehoon – kuva on piirretty logaritmisella asteikolla. Stefan-

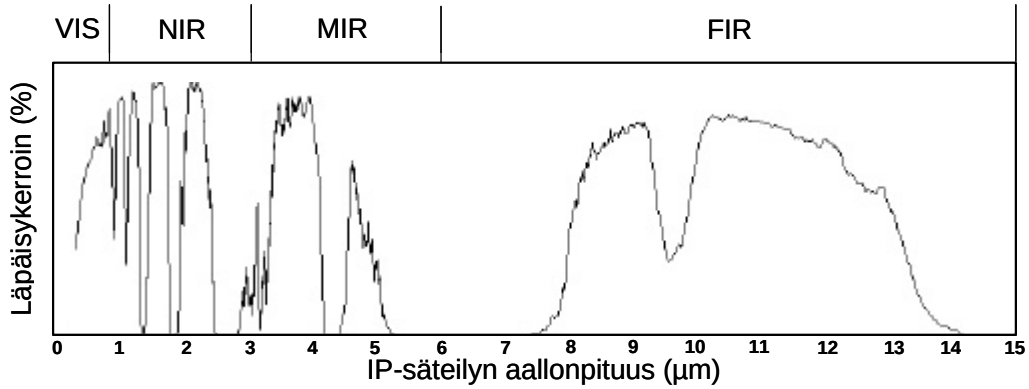
Bolzmannin laki kuvaa kappaleen säteilemän kokonaistehon riippuvuuden kappaleen lämpötilasta. Laki antaa säteilyteholle seuraavan lämpötilariippuvuuden:

$$W \propto T^4$$

missä $W$ on kappaleen säteilemä teho ja $T$ kappaleen lämpötila. Kappaleen lämpötilan (Kelvineinä) kaksinkertaistuessa lämpösäteilyn määrä siis 16-kertaistuu! Hyvin kuumia kappaleita on siten vaikea piilottaa häiveteknisesti, ja esim. lentokoneet turvautuvatkin harhauttavaan omasuojaan heittämällä soihtuja – lähestyvä ohjus pyritään houkuttelemaan kohti vielä kuumempaa eli voimakkaammin säteilevää maalia.

Kappaleen omien infrapunasäteilyominaisuuksien lisäksi infrapunasäteilyn hyödyntämiseen vaikuttavat keskeisesti ilmakehän läpäisyominaisuudet: ilmakehän kaasujen absorptio-ominaisuuksien vuoksi ilmakehä on läpinäkymätön tiettyjen aallonpituuksien infrapunasäteilylle, kun taas tietyille aallonpituusalueille ilmakehässä on ns. läpäisyikkunoita eli infrapunasäteily etenee ilmakehän läpi. Kuvassa L5.7 on esitetty ilmakehän läpäisy eri aallonpituuksille.

Kahdessa edellisessä kuvassa esitetyt lainalaisuudet muodostavat pohjan infrapunaalueen ELSO:lle: kappaleet säteilevät infrapunasäteilyä lämpötilasta riippuvalla aallonpituusjakaumalla ja teholla, ja osa tästä säteilystä pääsee ilmakehästä läpi. IP-sensorit ja -hakupäät toimivat näissä läpäisyikkunoissa, optimoituina kyseistä ikkunaa vastaavien lämpötilojen maaleille.




**Kuva L5.7: Esimerkki ilmakehän läpäisystä (transmittanssista) eri aallonpituuksilla. Läpäisykertoimen tarkat arvot riippuvat olosuhteista, esim. korkeudesta ja tarkasteluetäisyydestä, joten läpäisylle ei ole mahdollista antaa yhdessä kuvassa tai taulukossa tarkkoja arvoja. Olennaista on havaita, että joillakin aallonpituuksilla on läpäisyikkunoita, kun taas esim. 5,5-7,5 µm:n aallonpituuksilla ilmakehä on käytännössä läpinäkymätön.** [alkuperäisaineisto H. Ojansivu]

Edellä on esitetty tiivistetyssä muodossa elektronisen sodankäynnin kannalta keskeisiä teknisiä käsitteitä. Käsittely on luonnollisesti käytettävissä olevan sivumäärän ja kirjan

aihepiirin vuoksi pinnallista ja vain tärkeimpiin asioihin keskittyvää. Osaa keskeisimmistä käsitteistä on lisäksi syvennetty liitteissä 2 ja 3 elektronisen suojautumisen kannalta. Lisätietoa ELSO-tekniikasta voi lukea Maanpuolustus-korkeakoulun Tekniikan laitoksen digitaalista taistelukenttää ja elektronisen sodankäyntiä käsittelevistä julkaisuista.

# LIITE 6: HARJOITUSVASTUSTAJAN ELSO-JOUKOT

## Johdanto

Opetus- ja harjoituskäyttöön sekä julkisten opinnäytteiden lähdemateriaaliksi on eri maissa laadittu erilaisia harjoitusvastustajia. Suomen puolustusvoimissa käytössä on erilaisia harjoitusvastustajakuvauksia, jotka kaikki on tietoturvaluokiteltu, minkä vuoksi seuraavassa käsitellään julkisista lähteistä löytyviä amerikkalaisia kuvauksia. Tehtäessä luottamuksellista työtä on syytä käyttää hyväksi puolustusvoimien virallisia kuvauksia. Julkiset lähteet, erityisesti Internet, sisältävät lukuisia kuvauksia ELSO-joukoista, järjestelmistä ja niiden käytöstä. Tiedon suureen määrään sisältyy kuitenkin myös ongelma: oleellisen ja realistisen tiedon poimiminen edellyttää asiantuntija-analyysiä, mikä kuitenkin muuttaa tiedon helposti turvaluokitelluksi. Tästäkin syystä tämän kirjan harjoitusvastustajakuvaus on suora referaatti Yhdysvaltain armeijan käyttämästä vastustajasta. Lukijaa rohkaistaan tutustumaan Internetin tarjontaan myös ELSO:n alalla.

Kylmän sodan aikana länsimaiset harjoitusvastustajakuvaukset perustuivat Varsovan liiton sotavoimien muodostamaan uhkaan. Tällaisia kuvauksia olivat esim. brittien Generic Enemy Force (GENFORCE) ja Yhdysvaltain armeijan Opposing Force (OPFOR) FM 100-60-sarjan oppaissa. 1990-luvulla Varsovan liiton ja Neuvostoliiton hajottua uhkakuva muuttui kohti teknisesti kehittyneempää, mutta vähemmän massiivista skenaariota. Tässä liitteessä esiteltävä US Armyn 1990-luvun loppupuolen geneerinen vastustaja – josta käytetään nimeä OPFOR – jakautuu panssaroituihin ja mekanisoituihin joukkoihin sekä jalkaväkijoukkoihin[70]. Panssaroidut ja mekanisoidut joukot edustavat teknisesti kehittynyttä vastustajaa, kun taas jalkaväkijoukot kuvaavat yksinkertaisempaa ja kehittyvissä maissa kohdattavaa vastustajaa. OPFOR:n joukoista voidaan muodostaa monen mittakaavan kokonaisuuksia aina strategisia asejärjestelmiä omaaviin massiivisiin vastustajiin saakka.

OPFOR:ssa mainitut järjestelmät ovat yleensä venäläisiä. Dokumenteissa korostetaan kuitenkin ettei tarkoituksena ole osoittaa uhkakuvaksi mitään tiettyä maata, vaan niiden avulla ainoastaan luodaan konkreettinen mielikuva tietystä realistisesta suorituskyky-tasosta, sillä Neuvostoliiton runsaan aseviennin vuoksi kyseisiä järjestelmiä on laajassa käytössä maailmalla.

Uhkakuvan geneerisyyttä ei voi tässä yhteydessä liikaa korostaa – millään maalla ei ole täsmällisesti OPFOR:n kuvaamia joukkoja. Tämä liite on tarkoitettu ainoastaan antamaan mielikuva taistelukentällä toimivista ELSO-joukoista, ja nimenomaan maavoimien näkökannasta. Seuraavassa käsitellään teknisesti kehittyneen vastustajan panssaroituja ja mekanisoituja joukkoja (FM 100-60). Jalkaväkeen perustuvia joukkoja ei erikseen käsitellä, mutta ne sisältävät pitkälti samoja elementtejä.

Field Manual 100-61 kuvaa hyvin yksityiskohtaisesti geneerisen vastustajan operaatiotaitoa sisältäen informaatiosodankäynnin sekä tiedustelun ja elektronisen sodankäynnin toiminnan ja organisoinnin. Kokonaisuutta ei ole mahdollista käsitellä tässä yhteydessä, ainoastaan pinnallisesti ELSO-osia, mutta keskeinen ajatus OPFOR:n toiminnassa on nimenomaan käyttää taistelun eri elementtejä yhteisen tavoitteen saavuttamiseksi. Tässä yhteydessä tehty pelkkien ELSO-elementtien käsittely jättää siten kokonaisuuden hyvin vajavaiseksi.

## Elektroninen sodankäynti vastustajan informaatio-operaatioissa

OPFOR on kehittänyt pitkään systemaattisesti informaatiosodankäyntikykyään. Informaatiosodankäynti käsitetään jatkuvana ja sekä offensiivisena että defensiivisenä toimintana kaikissa sotatoimissa. Sen avulla saavutetaan informaatioylivoima kriittisinä ajanhetkinä ja kriittisissä paikoissa ja pakotetaan vastustaja reaktiiviseksi. OPFOR:n IW-doktriini käsittää useita elementtejä, joista ”operaatiot sähkömagneettisessa spektrissä”[ww] edustavat tässä kirjassa kuvattua länsimaista käsitystä ELSO:n informaatiosodankäyntiin kuuluvista elementeistä. Elektroninen taistelu on informaatiosodankäynnin keskeisin osa-alue, joka tukee jossain määrin kaikkia muita informaatiosodankäynnin elementtejä. Muista elementeistä mm. suojaus- ja turvallisuustoiminta, harhautus ja fyysinen tuhoaminen liittyvät elimellisesti ELSO:on – OPFOR käyttääkin näitä toimintoja tehokkaasti vahvistamaan ELSO:n vaikutusta.

***Harhautus*** on osa kaikkia OPFOR:n suunnitelmia ja sotatoimia, ja sen toteuttamiseen käytetään kaikkia mahdollisia keinoja, ml. multispektraalisia[xx] passiivisia ja aktiivisia elektronisia järjestelmiä. Esimerkiksi marssiosastojen todellinen koko ja reitti pyritään salaamaan harhamaalien (tutkaheijastin + IP-heräte) sekä viestiharhautus- ja tarvittaessa tutkahäirintälähettimien avulla. Harhautusta pyritään tekemään myös kaikilla sodankäynnin tasoilla – esim. häirintälähettimen avulla saatetaan muodostaa mielikuva uudesta asejärjestelmästä, jonka selvittämiseen vastustajan tiedustelujärjestelmä pyritään sitomaan.

Yksi OPFOR:n keskeinen toimintamalli on ***strateginen ELSO-tuli-isku***, jossa tärkeät kohteet pyritään tuhoamaan tai lamauttamaan ELSO:n ja fyysisen asevaikutuksen yhdistelmällä koko vastustajan syvyydessä. Isku pyritään toteuttamaan yllätyksenä

[ww] OPFOR-termeistä pääosa on käännetty vastaamaan suomalaista terminologiaa, minkä seurauksena kaikki käännökset eivät ole kirjaimellisia, toisaalta osassa on haluttu säilyttää täsmällisempi alkuperäinen merkitys. Esimerkiksi alkuperäistekstin ”elektroninen taistelu” on käännetty elektroniseksi sodankäynniksi. Kyseessä on kuitenkin suomalaista ELSO:a laajempi käsite, joka kattaa myös ELSO:n kohteiden fyysisen tuhoamisen.

[xx] Multispektraalisella tarkoitetaan useilla spektrin alueilla, kuten infrapuna- ja ultraviolettialueilla, samaan aikaan toimivaa.

ajan, kohteiden tai käytettävien menetelmien suhteen, massiivisena ja mahdollisimman useiden erilaisten asejärjestelmien avulla.

Toinen OPFOR:n toimintamalli on muodostaa ***tiedustelutuli-iskuja***, joissa integroidaan tiedustelu-, maalinosoitus-, tulenjohto- ja asejärjestelmät automaattiseksi kokonaisjärjestelmäksi, joka kykenee havaitsemaan ja tuhoamaan kriittiset maalit minuuteissa. Tällainen toimintamalli on käytössä mm. tykistön, raketinheittimistön ja tykistöohjusten, kaukoilmatoiminnan, hävittäjä- ja helikopteritoiminnan sekä elektronisen vaikuttamisen tulenjohdossa, joiden maalinosoitus pyritään saamaan lähes reaaliaikaiseksi. Kokonaisuuteen osallistuvien joukkojen ei tarvitse olla asejärjestelmälle alisteisina, vaan ne verkotetaan ainoastaan toiminnan ajaksi. Sensoreina voidaan käyttää kaikkia taistelukentän sensorijärjestelmiä. Esimerkkinä kuvataan, että hyvässä tilanteessa tykistön asevaikutus voi olla maalissa 2-4 minuutin kuluessa maalin havaitsemisesta.

***Tiedustelu*** on OPFOR:ille tärkein taistelua tukeva elementti. Tiedustelun tärkeimmät kohteet vaihtelevat strategisella, operatiivisella ja taktisella tasolla. Taktisen tason yhtymien ELSO-joukot pyrkivät paikantamaan vastustajan tärkeimmät johtamisyhteydet, ylemmillä organisaatiotasoilla tärkeäksi tulee saada kokonaiskuva vihollisvoimasta, jotta vastustajan neutralointiin tarvittavat joukot voidaan määrittää luotettavasti.

Armeijaryhmän keskeisimpiä tiedustelukohteita ovat:

- täsmäaseet
- joukkotuhoaseet (NBC)
- ilmapuolustusjärjestelmä
- tiedustelujärjestelmät
- ylemmät johtoportaat ja viestikeskukset
- ylemmän johtoportaan tykistöjoukot
- operatiivis-strategiset joukot ja niiden liikkeet

Armeijan ja armeijakunnan prioriteetteja edellisten lisäksi ovat:

- lentotukikohdat
- reservien keskitysalueet
- eri yksiköiden rajat
- puolustusalueiden sijainti ja laajuus
- vastustajan taistelukyky ja suunnitelmat

Divisioonien keskeisiä tiedustelukohteita ovat edellisten lisäksi:

- taistelussa kohdattavan joukon epäsuoran tulen yksiköiden ja taisteluhelikoptereiden sijainti
- panssari- ja panssarintorjuntajoukkojen sijoittelu
- ilmapuolustuksen ryhmitys
- prikaatien ja pataljoonien komentopaikat
- maasto

- taistelukentän puolustusjärjestelyt

Näiden kohteiden tiedusteluun ja maalittamiseen OPFOR käyttää myös elektronisen tuen yksikköjä.

## Elektronisen sodankäynnin toteuttaminen

OPFOR käsittelee ***elektronista taistelua***, johon kuuluu elektronisen tuen, vaikuttamisen ja suojautumisen lisäksi myös fyysinen tuhoaminen sekä signaalitiedustelu ja elektroninen vastatiedustelu. Fyysinen vaikuttaminen on ensisijainen menetelmä vastustajan viestiyhteyksien ja tutkien lamauttamiseksi. Sitä käytetään myös vastustajan

- täsmäasejärjestelmiä
- johtamisjärjestelmiä
- tykistö- ja ilmapuolustusjoukkoja
- elektronisen sodankäynnin järjestelmiä
- tiedustelu-, valvonta- sekä maalinosoitusjärjestelmiä vastaan.

Fyysinen tuhoaminen voidaan toteuttaa epäsuoran tulen, maahyökkäyksen tai lentorynnäkön avulla. Elektroninen vastatiedustelu käsittää vastustajan elektronista tiedustelua vaikeuttavat toimet, joihin kuuluvat erilaiset elektroniseen suojautumiseen liittyvät keinot ja harhautustoiminta. OPFOR korostaa voimakkaasti elektronista vastatiedustelua kriittisenä edellytyksenä etulyöntiaseman ja siten voiton saavuttamisessa.

OPFOR:n elektronisen sodankäynnin päämääränä on:

- havaita vastustajan elektroniset järjestelmät
- saattaa vastustajan johtamisjärjestelmät sekasortoon
- lamauttaa, kaapata tai tuhota vastustajan johtamisjärjestelmät
- heikentää vastustajan tiedustelua ja järjestelmiä
- suojella omia elektronisia yksiköitä ja järjestelmiä

***Elektronisessa taistelussa integrointi ja suunnittelu on kriittistä***. Suunnitteluprosessissa painotetaan hyvin tiukkaa koordinointia tiedustelun, elektronisen sodankäynnin ja operaatioiden suunnittelun välillä. Tämä takaa riittävän häirintä- ja muun tuen taistelujoukoille taistelun kriittisimmissä vaiheissa ja tärkeissä toimintasuunnissa. Se myös mahdollistaa vastustajan johtamisen tilapäisen lamauttamisen haluttuna hetkenä yhdistetyllä ase- ja häirintävaikutuksella. Myös tiedustelun ja häirinnän suhde koordinoidaan: vastustajan viestiliikennettä seurataan ja saatavia tietoja hyödynnetään, kunnes viestiverkon lamauttaminen tai tuhoaminen parhaiten tehostaa kokonaistilannetta.

OPFOR maalittaa vastustajansa elektronisen sodankäynnin järjestelmät, johtamis-järjestelmät sekä tiedustelujärjestelmät ELSO-tuli-iskun kohteeksi. Maalien priorisointijärjestys riippuu taistelun vaiheesta. Maalien tärkeysjärjestys on yleensä seuraava:

- täsmä- ja joukkotuhoaseet (NBC)
- johtamisjärjestelmät
- tykistöyksiköt, lento- ja ilmapuolustusyksiköt
- tiedustelusensorit ja tutkajärjestelmät
- taisteluun osallistuvat liikkuvat joukot
- reservit
- huoltokeskukset
- omaa etenemistä uhkaavat pistekohteet

Vaikka OPFOR on perinteisesti käyttänyt huippuunsa kehitettyjä sotilaallisia ELSO-järjestelmiä, se voi myös hyödyntää kaupallisia suhteellisen halpoja järjestelmiä. OPFOR sijoittaa ELSO-järjestelmänsä yleensä panssaroituihin tela-ajoneuvoihin mahdollistaen joukon mukana liikkumisen.

## ELSO:n elementtien käyttö taistelussa

### Elektroninen tuki

OPFOR ei erottele toisistaan taistelukentän signaalitiedustelua ja elektronista tukea. Siten edellä kuvattu tiedustelun priorisointiperiaate koskee myös elektronista tukea. Signaalitiedustelu nähdään yleisempänä käsitteenä, joka kattaa kaikki vastustajan emissioiden tunnistukseen, paikantamiseen ja niiden luonteen selvittämiseen liittyvät toimet.

OPFOR käyttää elektroniseen tukeen seuraavia joukkoja ja järjestelmiä:

- ilmavoimien signaalitiedustelujärjestelmiä
- armeijaryhmien, armeijoiden, armeijakuntien ja divisioonien signaali-tiedusteluyksiköitä
- maavoimien häirintäyksiköiden signaalitiedustelujärjestelmiä

Elektronisen tuen yksiköissä on asiantuntijoita signaalianalyysin ja kohteiden teknisen analyysin suorittamiseen sekä tärkeimpien tuhottavien, häirittävien, tai harhautettavien kohteiden maalittamiseen tai toimittamiseen tarkemmin analysoitavaksi.

OPFOR:n hyökkäyksen aikana elektronisen tuen järjestelmät ovat tyypillisesti hyökkäävän pääjoukon mukana, mahdollisimman edessä hyökkäyskärjessä. Puolustuksessa järjestelmät pyritään ryhmittämään turvalliselle vyöhykkeelle.

Tarvittaessa pääpuolustusalueelle ryhmitettynä järjestelmät sijoitetaan kärkiprikaatien kärkipataljoonien taakse. Kaikessa ryhmityksessä pyritään saamaan hyvä näköyhteys oletettuun toiminta-alueeseen. Joukkojen ryhmitystä muutetaan säännöllisesti, jotta kyetään suojautumaan vastustajan vastatoiminnalta.

OPFOR:n kyvyksi siepata ja suuntia *maasta käsin* vastustajan lähettimet on ilmoitettu seuraavia etäisyyksiä:

- Tykistön ja ilmapuolustuksen tutkajärjestelmät noin 25-50 km.
- VHF/UHF-alueen järjestelmät lähetystehosta riippuen noin 30-80 km.
- HF-pinta-aaltojärjestelmät yli 80 km etäisyydeltä hyökkäyskärjen tasalta mitattuna.
- HF-avaruusaaltojärjestelmien suuntimisetäisyys on periaatteessa rajoittamaton.
- Lentokonetutkien ja -viestijärjestelmien suuntimisetäisyys on radiohorisontin rajoissa.

OPFOR käyttää myös lentäviä tiedustelujärjestelmiä, jotka mahdollistavat edellä kuvattuja olennaisesti pidemmät tiedusteluetäisyydet. OPFOR:lla ei ole kunnollista hajaspektriradioiden tiedustelukykyä, mutta kylläkin erikoisjärjestelmiä kyseisten lähetteiden suuntimiseen.

OPFOR:n elektronisen tuen järjestelmien suuntimistarkkuus riittää tykistön maalinosoitukseen; tyypilliseksi paikantamistarkkuudeksi esimerkiksi tutkia vastaan on ilmoitettu 50-200 m. OPFOR:n vanhemmilla järjestelmillä maalinosoitusta varten tarvittiin vastustajalta vähintään 25 sekunnin lähetysjakso, uudemmilla järjestelmillä nämä aikarajat ovat huomattavasti lyhyempiä.

OPFOR on myös ryhtynyt käyttämään kaupallisia (COTS) järjestelmiä, joiden avulla voidaan saavuttaa huomattavaa suorituskykyä suhteellisen pienillä kustannuksilla.

## Elektroninen vaikuttaminen

***Elektronisen vaikuttamisen*** järjestelmiä modernisoidaan jatkuvasti vastustajan järjestelmien kehitystä seuraten. Häirintäjärjestelmät pyritään tekemään taistelunkestäviksi lisäämällä liikkuvuutta ja käyttämällä etukäteen tiedusteltuja ja valmisteltuja häirintäasemapaikkoja. Häirintää suoritetaan tavanomaisesti HF-, VHF-, UHF- ja tutkataajuuksilla, minkä lisäksi keskeisimpiä kohteita suojataan tykistötulelta lähisytyttimien häirintäjärjestelmillä.

Häirinnällä pyritään myös pakottamaan salattu viestiliikenne selkokieliseksi, tai pakotetaan vastustaja lähettämään pidempiä jaksoja, jotta suuntiminen tulisi mahdolliseksi. Häirintäjärjestelmien vastaanottimia käytetään elektronisen tuen tukena, kun häirintätehtävä ei ole käynnissä. Häirintälähettimiä myös käytetään suojaamaan

omia viestiyhteyksiä vastustajan häirinnältä lähettämällä peittävää häirintää vastustajan suuntaan.

Lennokkirykmentin lennokeissa voi olla signaalitiedustelu- tai häirintähyötykuormia, joiden avulla kohteen lähelle päästään helposti ja pienin riskein. Pieni häirintäteho ja lennokkijärjestelmien kapea taajuuskaista ovat kuitenkin ongelmia, joiden seurauksena lennokeilla häiritään tyypillisesti etukäteen valittuja kohteita.

OPFOR pyrkii yllätykseen häirintätoiminnassaan, esim. alistamalla käyttöön oleellisesti enemmän maa- ja ilmasijoitteista häirintää kuin osattaisiin olettaa. Sen tavoitteena on lamauttaa vastustajan ilmapuolustus ennen rynnäkkö- ja pommikoneiden tunkeutumista syvälle vastustajan alueelle. Tunkeutumiskäytävät ovat kapeita, tyypillisesti 10-15 km leveitä sektoreita. Jokaisen armeijaryhmän toiminta-alueelle luodaan tyypillisesti yksi tai kaksi käytävää yhdistämällä elektronista ja fyysistä asevaikutusta vastustajan tutkia ja ilmatorjuntaohjusjärjestelmiä vastaan. OPFOR hyökkää ensin vastustajansa ilmavalvonta- ja taistelunjohtotutkia sekä ilmapuolustuksen keskeisimpiä viestijärjestelmiä vastaan käyttäen taustahäirintää sekä massiivista silputusta (jopa 36 km x 360 km, kesto useita tunteja). Mikäli tämä vaihe onnistuu hyvin, vaikeammin häirittävät tulenjohtotutkat joutuvat toimimaan itsenäisesti, ilman datafuusion antamaa tukea, ja tausta-, saatto- sekä omasuojahäirinnän häiritseminä, minkä seurauksena koordinoimaton tulenkäyttö johtaa nopeasti ohjusten ja ammusten loppumiseen huonolla hyötysuhteella. Vastustajan ilmapuolustuksen lamauttamiseen voi liittyä myös harhautus esimerkiksi lennokeilla toteutetuin simuloiduin hyökkäyksin. Vastustajan käynnistäessä harhautushyökkäyksen torjunnan, sen ilmanpuolustusjärjestelmä paljastuu hyökkääjän elektroniselle tiedustelulle, jolloin sen tuhoaminen esimerkiksi tutkasäteilyyn hakeutuvin ohjuksin on mahdollista. Ilmapuolustuksen lamauttamiseen liittyen maavoimat pyrkivät tuhoamaan kaikki ballististen ohjusten, tykistön ja raketinheittimistön kantaman sisäpuolella olevat ilmapuolustusasejärjestelmät ja -tutkat.

OPFOR pyrkii vahventamaan omaa ilmapuolustustaan hyödyntämällä häirintäjärjestelmiä ja halpoja passiivisia menetelmiä kuten tutkaharhamaaleja, joiden seurauksena vastustaja pakotetaan toisaalta muuttamaan lentoprofiilejaan (esim. häiritsemällä maastonseurantatutkaa tai tutkakorkeusmittaria) ja siten joutumaan ilmatorjunnan vaikutusalueelle. Häirinnällä yritetään myös murtaa maalinseurantalukitus.

Armeijaryhmän ilmapuolustushäirintärykmenttiä käytetään ilma-alusten maastonseuranta-, navigointi-, rynnäkkötutka- ja tiedustelujärjestelmiä vastaan. Rykmentin tiedustelujärjestelmiä käytetään antamaan maalitietoa häirintäjärjestelmille. Häirintäjärjestelmiä käytetään myös puolustamaan omia kriittisiä kohteita, kuten lentotukikohtia, huoltokeskuksia, tärkeimpiä viestiyhteyksiä ja ylempiä komentopaikkoja.

OPFOR:n maajoukkojen päähäirintämenetelmiä ovat:

- tutkien kapea- ja laajakaistainen sekä taajuudessa pyyhkäisevä häirintä, pulssihäirintä, silput ja harhamaalit,

- AM- ja FM-viestiliikenteen kapea- ja laajakaistainen sekä taajuudessa pyyhkäisevällä häirintä
- komento-ohjausjärjestelmien häirintä

Maajoukot voivat saada kansallisen tason häirintäyksiköitä käyttöönsä, jolloin niiden maa- ja lentokonesijoitteisen häirintäjärjestelmien häirintäkyky kattaa mm. maalinosoitustutkien, aseiden ohjausjärjestelmien ja lentokoneiden navigointijärjestelmien häirinnän, sekä harhamaalien luonnin vastustajan ilmapuolustusjärjestelmään.

## Elektroninen suojautuminen

Elektronista suojautumista korostetaan huomattavasti mm. viestiliikennekurin, emissiokontrollin, päällekkäisten varajärjestelmien, järjestelmäsuunnittelun, henkilöstön ammattitaidon, herätteiden pienentämisen, salausjärjestelmien ja vaihtoehtoisten viestijärjestelmien avulla. Esimerkiksi suuretkin joukkojen siirrot pitää kyetä suorittamaan täydellisessä elektronisessa hiljaisuudessa. Esimerkkeinä elektronisen suojautumisen menetelmistä voidaan mainita ilmapuolustuksessa käytettävän mm. seuraavia:

- Aisti-ilmavalvonta ja muut sensorit täydentävät tutkailmavalvontaa.
- Ylempien yksikköjen ilmavalvontatutkat osoittavat maalit suoraan ilmapuolustusjoukoille, mikä suojaa it-yksiköiden tutkia paljastumiselta ja tuhoamiselta.
- Emissioiden hallinta on ohjattua ja sen noudattamiskuri tiukka.
- Laajan taajuuskaistan käyttäminen. Kaikissa ilmapuolustusjärjestelmissä on tutkia useilla taajuusalueilla, joten yhdellä häirintäjärjestelmällä ei voida häiritä koko järjestelmää.
- Tutkien taajuudenhypytystä käytetään häirinnän väistämiseen.
- Viestiliikennettä suojataan tiedustelulta ja sen seurauksena häirinnältä myös oman liikenteen peittävällä (maskaavalla), vastustajan suuntaan kohdistetulla häirinnällä
- Samoissa asejärjestelmissä on useita vaihtoehtoisia ilmatorjuntaohjusten ohjausjärjestelmiä (erilaisia tutkia, optiset näkyvän valon ja infrapunajärjestelmät), jolloin vastustajan kyetessä häiritsemään yhtä hakeutumismenetelmää voidaan käyttää jotakin toista hakeutumismenetelmää.
- Ase- ja sensorijärjestelmiä suojataan myös liikkeellä.

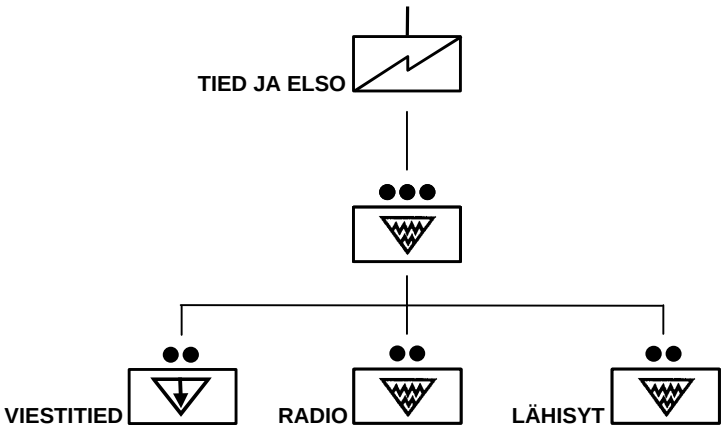
# ELSO-joukot OPFOR:n organisaatioissa

## Prikaatin orgaaniset ELSO-joukot

OPFOR:n pataljoonissa ja sitä pienemmissä yksiköissä ei ole omaa ELSO-kykyä. Prikaatit (tai rykmentit) kuuluvat joko divisiooniin tai toimivat erillisinä. Divisiooniin kuuluvissa prikaateissa ei ole omia ELSO-yksiköitä. Erillisiin prikaateihin kuuluu ***tiedustelu- ja ELSO-komppania***, joka käsittää tavanomaisten tiedustelujoukkueiden lisäksi elektronista sodankäyntiä suorittavan ***häirintäjoukkueen***. Häirintäjoukkueen ELSO-voima jakaantuu viestitiedustelu-, radiohäirintä- ja lähisytyttimien häirintäryhmiin. Häirintäjoukkueen kalustona on:

- 3 x Tiedusteluvastaanotin/suuntimojärjestelmä
- 3 x VHF-häirintäjärjestelmä
- 1 x HF-häirintäjärjestelmä
- 3 x Lähisytyttimien häirintäjärjestelmä

Elektronisen sodankäynnin kalustot on yleensä asennettu panssaroituihin ajoneuvoihin.




**Kuva L6.1: Erillisen prikaatin ELSO-voima on sijoitettu tiedustelu- ja ELSO-komppaniaan.**

## Divisioonan orgaaniset ELSO-joukot

Mekanisoituun jalkaväkidivisioonaan ja panssaridivisioonaan kuuluu tyypillisesti ***tiedustelu- ja ELSO-pataljoona***. Pataljoonaan kuuluu tavanomaisten tiedustelukomppanioiden lisäksi signaalitiedustelukomppania ja häirintäkomppania.

***Signaalitiedustelukomppaniaan*** kuuluu viestitiedustelu- ja -suuntimojoukkue, sekä vastaavasti tutkien tiedustelu- ja suuntimojoukkue (suomalaisin termein elektronisen

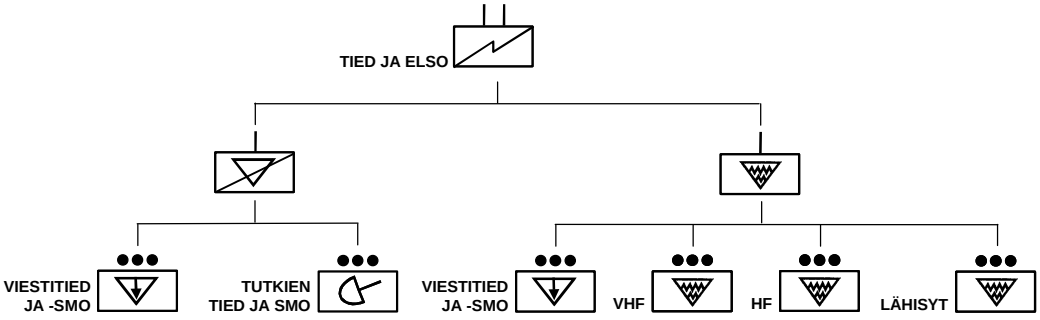
mittaustiedustelun joukkue). Signaalitiedustelukomppanian elektronisen sodankäynnin järjestelmät ovat:

- 7 x HF/VHF-tiedusteluvastaanotin/suuntimojärjestelmä
- 3 x Tutkien tiedusteluvastaanotin/suuntimojärjestelmä

***Häirintäkomppaniaan*** kuuluu viestitiedustelu- ja suuntimojoukkue, VHF-häirintäjoukkue, HF-häirintäjoukkue sekä lähisytyttimien häirintäjoukkue. Komppanian käytössä ovat seuraavat järjestelmät:

- 3 x HF/VHF-tiedusteluvastaanotin/suuntimojärjestelmä
- 3 x VHF-häirintäjärjestelmä
- 1 x HF-häirintäjärjestelmä
- 3 x Lähisytyttimien häirintäjärjestelmä

Tiedustelu- ja ELSO-pataljoonaan saattaa kuulua myös ***lennokkilaivue***, jonka kalustona on kahdeksan kauko-ohjattavaa lennokkia ja neljä niiden ohjausyksikköä. Vaikka tätä lennokkilaivuetta ei varsinaisesti kuvatakaan ELSO-joukkona, voidaan lennokit varustaa ELSO-hyötykuormin (elektroninen tuki tai vaikuttaminen). Lennokkilaivue voi kuulua myös armeijan tai armeijaryhmän alaiseen maalinosoitusrykmenttiin.



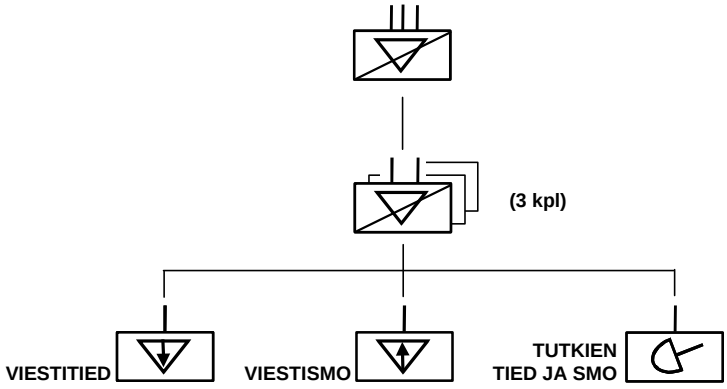

**Kuva L6.2: Divisioonan tiedustelu- ja ELSO-pataljoona sisältää signaalitiedustelukomppanian sekä häirintäkomppanian.**

## Armeijakunnan ja armeijan ELSO-joukot

OPFOR:n armeijakunnilla ja armeijoilla ei ole kiinteää kokoonpanoa, vaan se riippuu tilanteesta, tehtävästä ja toiminta-alueesta. Armeijakuntaan voi kuulua signaalitiedustelupataljoona ja/tai häirintäpataljoona. Armeijaan kuuluu 1-2 signaalitiedustelupataljoonaa tai vaihtoehtoisesti signaalitiedustelurykmentti, sekä yksi häirintäpataljoona tai -rykmentti. ***Signaalitiedustelurykmenttiin*** kuuluu kolme signaalitiedustelupataljoonaa ja ***häirintärykmenttiin*** kolme häirintäpataljoonaa.

***Signaalitiedustelupataljoonaan*** kuuluu ELSO-osina viestitiedustelukomppania, viestisuuntimokomppania sekä tutkien tiedustelu- ja suuntimokomppania. Signaalitiedustelupataljoonan ELSO-kalusto on:

- 12 x Viestitiedustelujärjestelmä
- 9 x Viestisuuntimojärjestelmä
- 9 x Tutkien tiedusteluvastaanotin/suuntimojärjestelmä




**Kuva L6.3: Armeijan signaalitiedustelurykmentti käsittää kolme signaalitiedustelupataljoonaa, joihin kuhunkin kuuluu viestitiedustelukomppania, viestisuuntimokomppania sekä tutkien tiedustelu- ja suuntimokomppania. Signaalitiedustelupataljoona voi kuulua myös armeijakunnan alaisuuteen.**

Armeijakunnille ja armeijoille alisteisissa signaalitiedustelupataljoonissa korostuu VHF-alueen viestitiedustelu- ja suuntimojärjestelmien osuus. HF-alueen järjestelmiä on enemmän armeijaryhmillä.

***Häirintäpataljoonan*** ELSO-osia ovat viestitiedustelu- ja suuntimokomppania, 1-2 VHF/UHF-häirintäkomppaniaa, HF-häirintäkomppania sekä lähisytyttimien häirintäjoukkue. Armeijakunnalla on tyypillisesti yksi VHF/UHF-häirintäkomppania, armeijalla kaksi. Häirintäpataljoonan ELSO-kalusto on:

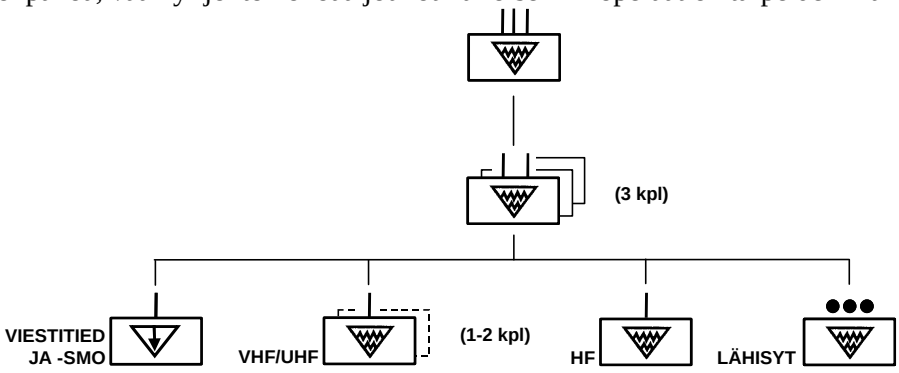
- 3 x VHF-tiedusteluvastaanotin/suuntimojärjestelmä
- 3 x HF-tiedusteluvastaanotin/suuntimojärjestelmä
- 9 (armeijakunta) / 18 (armeija) x VHF-viestihäirintäjärjestelmä
- 3 (armeijakunta) / 6 (armeija) x UHF-viestihäirintäjärjestelmä
- 9 x HF-viestihäirintäjärjestelmä
- 3 x Lähisytyttimien häirintäjärjestelmä

Armeijakunnan ja armeijan alaisuuteen kuuluu myös ***lennokkilaivue***, jonka kalustona on 12 reitilleen etukäteen ohjelmoitavaa lennokkia. Vaikka tätä lennokkilaivuetta ei

varsinaisesti kuvatakaan ELSO-joukkona, se voidaan varustaa myös ELSO-hyötykuormalla.

### Armeijaryhmän ELSO-joukot

OPFOR käyttää nimitystä ”armeijaryhmä” korkeimman tason organisaatiosta, jolla suoritetaan sotanäyttämöllä strategisia operaatioita. Armeijaryhmällä ei ole kiinteää kokoonpanoa, vaan ylijohto kokoaa joukot kulloisenkin operaation tarpeiden mukaan.

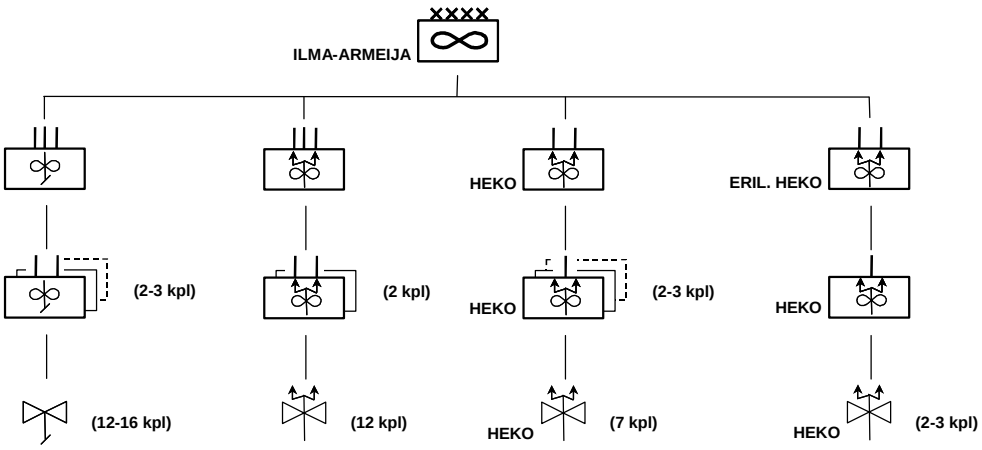



**Kuva L6.4: Armeijan häirintärykmentti käsittää kolme häirintäpataljoonaa, joihin kuhunkin kuuluu häirintämaalit määrittävä ja niitä seuraava viestitiedustelu- ja suuntimokomppania, 1-2 VHF/UHF-häirintäkomppaniaa, HF-häirintäkomppania ja herätesytytinten häirintäjoukkue. Häirintäpataljoona voi kuulua myös armeijakunnan alaisuuteen.**

Armeijaryhmään voi kuulua seuraavia yksiköitä, joilla on omaa ELSO-suorituskykyä:

- Ilma-armeija
- Ilmapuolustushäirintärykmentti
- Lennokkirykmentti
- 1-2 signaalitiedusteluprikaatia (toisen tilalla voi olla signaalitiedustelurykmentti tai erillinen pataljoona)
- Häirintärykmentti tai -pataljoona

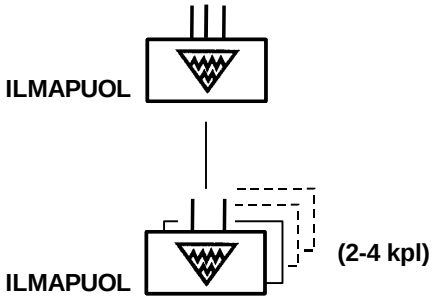
***Ilma-armeija*** on liukuva organisaatio. Siihen voi kuulua tuettavien maajoukkojen tarpeiden mukaan ELSO-komponentteja sisältävät tiedustelulentorykmentti ja häirintähelikopterilaivue, sekä mahdollisesti häirintälentorykmentti ja erillinen helikopterilaivue.




**Kuva L6.5: OPFOR:n ilma-armeijan ELSO-voima.**

***Tiedustelulentorykmenttiin*** kuuluu 2-3 tiedustelulentolaivuetta, joista kunkin kalustona voi olla 12-16 kpl tiedustelukonetta. Käytössä on lukuisia erilaisia sensorikokonaisuuksia, myös elektronisen tuen sensoreita. ***Häirintälentorykmenttiin*** kuuluu kaksi häirintälentolaivuetta, joista toisen kalustona voi olla 12 kpl häirintäkonetta. ***Häirintähelikopterilaivueessa*** on 2-3 häirintähelikopterilentuetta, joissa on yhteensä 14-21 kpl häirintähelikopteria. Häirintähelikopterilentue voi joskus kuulua 2-3 häirintähelikopterin vahvuudella myös ilma-armeijan alaiseen erilliseen helikopterilaivueeseen. Kyseisessä laivueessa on muiden helikopterilentueiden lisäksi myös tiedusteluhelikopterilentue, jonka sensoreina kuitenkin viitataan ainoastaan NBC-näytteenottoon ja kuvaustiedusteluun.

***Ilmapuolustushäirintärykmentti*** koostuu 2-4 ilmapuolustushäirintäpataljoonasta, joista osa on tyypillisesti alistettu armeijaryhmän päätoimintasuunnan armeijakunnille tai armeijoille, ja loput asetettu suojaamaan armeijaryhmän tärkeimpiä yksiköitä. Kullakin pataljoonalla voi olla jopa 54 ilmapuolustushäirintälähetintä sekä niihin liittyvät maalinosoitusjärjestelmät.



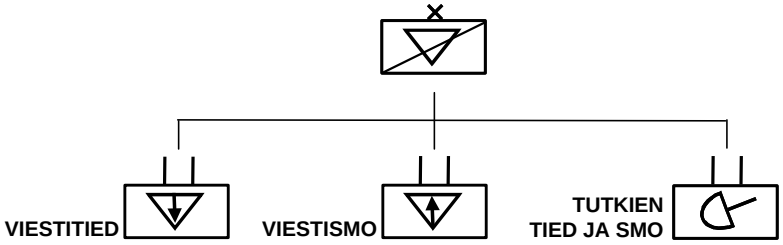

**Kuva L6.6: Ilmapuolustushäirintärykmentti, jolla voi olla jopa yli 200 ilmapuolustukseen liittyvää häirintälähetintä**

***Lennokkirykmentti*** koostuu kolmesta lennokkilaivueesta, joissa on yhteensä 24 kauko-ohjattavaa tai reitilleen etukäteen ohjelmoitavaa lennokkia, 12 niiden lähetysajoneuvoa ja 6 ohjausasemaa. Lennokkirykmentin lennokkeihin voidaan asentaa myös elektronisen tuen tai vaikuttamisen järjestelmiä.

***Signaalitiedusteluprikaatin*** ELSO-osia ovat viestitiedustelupataljoona, viestisuuntimopataljoona sekä tutkien tiedustelu- ja suuntimopataljoona. Signaalitiedusteluprikaati vastaa kalustoltaan pitkälti em. signaalitiedustelurykmenttiä, mutta jako

pataljooniin on poikkeava: rykmentissä pataljoonat ovat identtisiä, prikaatissa kullakin on oma erityinen rooliinsa. Signaalitiedusteluprikaatin ELSO-kalusto on:

- 36 x Viestitiedustelujärjestelmä
- 27 x Viestisuuntimojärjestelmä
- 27 x Tutkien tiedusteluvastaanotin/suuntimojärjestelmä
-




**Kuva L6.7: Signaalitiedusteluprikaati sisältää mm. viestitiedustelupataljoonan, viestisuuntimopataljoonan sekä tutkien tiedustelu- ja suuntimopataljoonan.**

## Muut ELSO-joukot

Yhdysvaltain maavoimien OPFOR-harjoitusvastustajakuvaus sisältää ainoastaan maavoimien taistelukentällä kohtaamat joukot, minkä vuoksi muiden puolustushaarojen toimintaan liittyvää ELSO:a ei ole juurikaan käsitelty. OPFOR:n kalustoon kuvataan kuuluvan useita erilaisia signaalitiedustelusatelliitteja, joiden avulla taistelukentän elektronista taistelujaotusta voidaan tiedustella. OPFOR myös kykenee satelliittitietoliikenteen häirintään.

# LIITE 7: KÄSITTEET JA MÄÄRITELMÄT

Seuraavassa on esitetty kirjassa esiintyvien elektronisen sodankäynnin termistö. Osa määritelmistä on kirjoittajien omia, koska kaikista termeistä ei ole olemassa määritelmää tai englanninkielistä määritelmää ei ole aiemmin suomennettu. Suomennoksissa on pyritty säilyttämään termin alkuperäiskielisen ilmaisun merkityssisältö, jotta termistö olisi kansainvälisesti yhteensopivaa.

**Aktiivinen elektroninen suojautuminen** (active electronic protection) tarkoittaa kaikkia niitä aktiivisia toimia, joilla pyritään peittämään omien elektronisten järjestelmien toiminta, takaamaan niiden toimintakyky vastustajan niihin kohdentaman elektronisen vaikutuksen alaisena ja joilla pyritään estämään niihin kohdistuva vastustajan asevaikutus.

**Elektroninen harhauttaminen** (electronic deception) tarkoittaa toimenpiteitä, joilla vaikeutetaan vastustajan kykyä tiedustella, paikantaa, seurata ja kohdistaa toimenpiteitä omia järjestelmiämme vastaan antamalla tarkoituksellisesti virheellistä tietoa. Vertaa *harhauttaminen*.

**Elektroninen hiljaisuus** (electronic silence) tarkoittaa Suomessa sitä, että kaikista sähkömagneettista säteilyä lähettävistä laitteista on oltava virta katkaistu tai ne on oltava niin suojattuja, ettei niiden lähettämää säteilyä voi ilmaista.

**Elektroninen häirintä** (electronic jamming) tarkoittaa toimenpiteitä, joilla vaikeutetaan tai estetään vastustajan sähkömagneettista säteilyä hyödyntävien järjestelmien käyttöä. Elektroninen häirintä jakautuu tavoitteena olevan vaikutuksen mukaan estävään ja harhauttavaan häirintään.

**Elektroninen lamauttaminen** (electronic destruction) käsittää toimenpiteitä, joilla vaurioitetaan sähkömagneettisella energialla joko tilapäisesti tai pysyvästi vastustajan elektronisia järjestelmiä.

**Elektroninen maalinosoitus** (electronic target acquisition) on passiivisin menetelmin tehtävää reaaliaikaista maalien etsintää ja paikantamista, jonka tavoitteena on asejärjestelmän tarvitsevan maalitiedon tuottaminen.

**Elektroninen mittaustiedustelu** (electronic intelligence, ELINT) on vastustajan sensori- ja navigointisignaaleihin sekä muihin viestijärjestelmiin kuulumattomiin signaaleihin kohdistuvaa signaalitiedustelua tai elektronista tiedustelua ja valvontaa.

**Elektroninen peittäminen** (electronic masking) tarkoittaa oman toiminnan suojaamista vastustajan elektroniselta tuelta peittämällä omien järjestelmien lähetteet sähkömagneettiseen spektriin.

**Elektroninen suojautuminen** (ELSU, electronic protection, EP) on se osa elektronisesta sodankäynnistä, jonka toimenpitein varmistetaan omien järjestelmien tehokas käyttö ottaen huomioon vastustajan elektroninen tiedustelu ja valvonta, vaikuttaminen ja suojautuminen. Elektronien suojautuminen jakautuu *teknisesti* 1) aktiiviseen ja 2) passiiviseen suojautumiseen sekä *operatiivisesti* 1) suojautumiseen vastustajan elektroniselta tiedustelulta ja valvonnalta ja sen ohjaamalta tulenkäytöltä sekä 2) suojautumiseen vastustajan elektroniselta vaikuttamiselta.

**Elektroninen tiedustelu ja valvonta** (electronic reconnaissance and surveillance) on vastustajan, omien joukkojen ja mahdollisten kolmansien osapuolten sensori-, navigointi- ja viestijärjestelmiin kohdistuvaa tiedustelua ja valvontaa, jonka tavoitteena on reaaliaikaisen elektronisen tilannekuvan luominen ja ylläpito sekä elektronisen maalinosoituksen ja uhkavaroituksen tukeminen. Vertaa *signaalitiedustelu*.

**Elektroninen tuki** (ELTU, electronic support, ES) tuottaa elektronisten lähetteiden ilmaisun ja mahdollisesti myös suuntimisen perusteella tilannekuvaa tai sitä täydentäviä tietoja. Se on reaaliaikaista tiedustelua ja valvontaa, joka kohdistuu vastustajan lisäksi omien joukkojen ja niiden toimintaympäristön sähkömagneettista säteilyä käyttäviin järjestelmiin. Elektroninen tuki jakautuu 1) elektroniseen tiedusteluun ja valvontaan, 2) elektroniseen maalinosoitukseen ja 3) elektroniseen uhkavaroitukseen.

**Elektroninen uhkavaroitus** (electronic threat warning) tarkoittaa järjestelmiä, joiden avulla voidaan havaita, paikantaa ja tunnistaa omiin järjestelmiin välittömästi kohdistuva tiedustelu ja asevaikutusuhka ja joiden antamien tietojen perusteella voidaan optimoida omat vastatoimet. Elektroninen uhkavaroitus muodostaa yleensä osan kohteiden omasuojajärjestelmää.

**Elektroninen vahvistaminen** (electronic hardening) tarkoittaa keinoja, joilla pyritään takaamaan omien elektronisten järjestelmien toimintakyky vastustajan niihin sähkömagneettisen spektrin avulla kohdistaman uhan alaisena. Keinoina voidaan käyttää esimerkiksi kotelointia, maadoitusta, suodattimia, vaimentimia yms. teknisiä keinoja.

**Elektroninen vaikuttaminen** (ELVA, electronic attack, EA) on se osa elektronisesta sodankäynnistä, joka käsittää kaikki ne toimenpiteet, joilla sähkömagneettisen spektrin välityksellä pyritään estämään, hidastamaan tai vähentämään vastustajan sähkömagneettista säteilyä hyödyntävien tai elektroniikasta riippuvien järjestelmien käyttöä. Elektroninen vaikuttaminen jakautuu (1) elektroniseen häirintään, (2) elektroniseen harhauttamiseen ja (3) elektroniseen lamauttamiseen.

**Elektroninen viestitiedustelu** (communications intelligence, COMINT) on vastustajan viestisignaaleihin kohdistuvaa signaalitiedustelua tai elektronista tiedustelua ja valvontaa.

**Elektronisen sodankäynnin tukitoiminta** (EW Support) käsittää ne toiminnat, joilla luodaan edellytykset elektroniselle suojautumiselle, tuelle ja vaikuttamiselle. Käsittää erityisesti signaalitiedustelun avulla tuotettujen signaalikirjastojen muokkauksen emitterikirjastoiksi, elektronisen sodankäynnin järjestelmien parametroinnin (evästyksen), operaatioiden tuen parametritietojen avulla sekä operatiivistaktisen tuen elektronisen sodankäynnin joukoille.

**Emissioiden hallinta** (emission control, EMCON) tarkoittaa sähkömagneettisen spektrin ajallisesti, alueellisesti ja taajuuskaistallisesti valikoitua ja operaatioajatukseen sekä operaatiovaiheeseen sidottua ohjattua ja valvottua sähkömagneettisen spektrin aktiivista käyttöä, jonka tavoitteena on estää vastustajaa saamasta tietoa operaatiosta, joukosta ja järjestelmistä elektronisen tuen keinoin tai tukea operatiivista harhauttamista.

**EMP-ase** (electromagnetic pulse weapon, EMP weapon) on konventionaaliseen räjähteeseen (siis ei ydinräjähteeseen) perustuva ase, joka synnyttää paikallisen radiotaajuisen sähkömagneettisen säteilypiikin, joka vaurioittaa kohteena olevan järjestelmän ja muiden kohdealueella olevien järjestelmien elektronisia komponentteja.

**Hajasäteilytiedustelu** (unintended radiation intelligence) on polttomoottoreiden sytytysjärjestelmistä sekä elektronisista laitteista lähtevän tahattoman sähkömagneettisen säteilyn perusteella tehtävää järjestelmien paikantamista sekä laitteiden ominaisuuksien ja käytön selvittämistä.

**Harhauttaminen** (deception) on väärän käsityksen antamista vastustajalle tuottamalla ja jakamalla harhauttavaa informaatiota sekä harhauttamiseen liittyvän oikean tiedon salaamista. Harhauttamisen tavoitteena on heikentää vastustajan päätöksentekokykyä joko hidastamalla tämän päätöksentekoa tai ohjaamalla tätä tekemään vääriä päätöksiä. Elektronisen sodankäynnin yhteydessä harhauttamisella tarkoitetaan järjestelmien sijainnin, liikkeen ja spektrin käytön peittämistä fyysisin harhamaalein ja sähkömagneettisin harhalähettein sekä järjestelmien käyttöasteen ja käyttötarkoituksen peittämistä harhauttavien lähettein. Suojaavalla harhauttamisella pyritään estämään järjestelmien kriittisten osien paljastuminen ja paikantaminen sekä vaikeuttamaan vastustajan asejärjestelmien maalin valintaa ja aseiden maaliin hakeutumista.

**Häivemenetelmät** (stealth measures) tarkoittavat keinoja, joilla pyritään minimoimaan suojattavien kohteiden emittoiman ja heijastaman säteilyn erot taustaansa nähden kaikilla sähkömagneettisen spektrin alueilla, kuten radio- ja tutkataajuuksilla, infrapuna-aallonpituuksilla sekä näkyvän valon ja ultraviolettisäteilyn alueella. Minimoitavia eroja ovat kohteen ja taustan välinen kontrasti, ääriviivojen luonne sekä pinnan kuviointi. Tutkataajuusalueella pyritään minimoimaan tutkapulssin heijastuminen ja sironta tutkavastaanottimen suuntaan.

**Informaatiohyökkäys** (information attack, IA) tarkoittaa toimia, joilla vaikutetaan tai lamautetaan vastustajan informaatiojärjestelmä ilman fyysistä vaikuttamista siihen tai sen ympäristöön.

**Informaatio-operaatio** (information operation, IO) on informaatiosodankäynnin osa-alueisiin perustuva sotilas- ja/tai siviilioperaatio.

**Informaatio-operaatioturvallisuus** (information operations security) on kokonais-operaatioon liittyvä informaatiosodankäynnin osa-alue, jonka tavoitteena on tunnistaa ja suojata omat kriittiset tiedot ja tietojärjestelmät sekä estää niiden paljastuminen vastustajalle. Katso *operaatioturvallisuus*.

**Informaatiosodankäynti** (information warfare, IW) on valtion yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja tältä suojautumista. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin strategisella, operatiivisella tai taktisella tasolla. Informaatiosodankäynti koskee koko yhteiskuntaa ja on siten luonteeltaan strategista toimintaa. Informaatiosodankäynnin keskeiset vaikuttamis- ja suojautumiskeinot ovat tietoverkkosodankäynti, elektroninen sodankäynti, psykologinen sodankäynti, fyysinen vaikuttaminen tiedustelu-, valvonta- ja johtamisjärjestelmään, operaatioturvallisuus ja harhauttaminen[yy].

**Informaatiouhka** on tahtoon, tietoon ja tietoa käsitteleviin henkilöihin ja järjestelmiin kohdistuvaa tahallista tai tahatonta toimintaa, joka voi heikentää informaation luotettavuutta, luottamuksellisuutta, eheyttä tai käytettävyyttä sekä ohjata mielipiteen muodostusta ja päätöksentekoa vastustajan haluamaan suuntaan erilaisin tietoteknisin, sähkömagneettisin, fyysisin tai psykologisin keinoin.

**Informaatioylivoima** (IS, Information Superiority) on suhteellinen ylivoima informaatio-operaatiossa vastustajaan nähden ajantasaisen informaation keräämisessä, käsittelemisessä ja jakamisessa. Informaatioylivoima saavutetaan sekä tukemalla omaa informaatioprosessia että heikentämällä vastustajan informaatioprosessia

**Johtamissodankäynti** (JOSO, command and control warfare, C2W) on asevoimien informaatiosodankäynnin sotilaallista toteuttamista poikkeusolojen aikana ja tämän toiminnan rauhanaikaista valmistelua. Termin kansainvälinen käyttö on vähenemässä ja sen vuoksi tulisi suosia nimitystä puolustusvoimien informaatiosodankäynti.

**Kielletyt taajuudet** (taboo frequencies) ovat omien elektronisten järjestelmien käyttämiä taajuuksia, joita ei saa missään tilanteessa häiritä, kuten kansainväliset hätätaajuudet ja turvallisuuteen vaikuttavat taajuudet.

[yy] Yllä suomalainen määritelmä. Joidenkin näkemysten mukaan informaatiosodankäynti on teoria, jota sovelletaan käytäntöön informaatio-operaatioissa. Zachary P. Hubbard: *IO in the Information Age*. Journal of Electronic Defense. Toukokuu 2004, s. 50.

**Kohdevaikutuksen arviointi** (battle damage assessment, BDA) tarkoittaa sotilaallisen voiman käytön toteutuneen vaikutuksen arviointia. Tässä yhteydessä käsite sotilaallinen voima käsittää sekä tappavat että ei-tappavat menetelmät, mukaan lukien elektronisen sodankäynnin ja informaatiosodankäynnin vaikutusmenetelmät. Kohdevaikutuksen arviointi käsittää fyysisen ja toiminnallisen vaikutusarvion.

**Kuuntelutiedustelu** on (elektronista) viestitiedustelua, jossa myös selvitetään ja kuunnellaan viestilähetteen sisältö.

**LPD-signaali** (low probability of detection) tarkoittaa signaalia tai järjestelmää, jonka signaali on vaikeasti ilmaistavissa, esimerkiksi osa FM/CW- ja hajaspektrilähetteistä.

**LPE-signaali** (low probability of exploitation) tarkoittaa signaalia tai järjestelmää, jonka signaali on ilmaisun jälkeen vaikeasti hyödynnettävissä (suunnittavissa, purettavissa, analysoitavissa tai tunnistettavissa).

**LPI-signaali** (low probability of intercept) tarkoittaa signaalia tai järjestelmää, jonka signaali on vaikeasti siepattavissa, esimerkiksi hyppivätaajuiset signaalit sekä purskelähetteet.

**Lähetyskielto** on Suomessa määritelty termi, joka tarkoittaa sitä, ettei radio- ja tutkalaitteilla saa lähettää.

**Lähihäirintä** (stand-in jamming) on tukihäirinnän laji, jossa häirintälähetin viedään hyvin lähelle häirittävää kohdetta. Häirintälähetin voi olla sijoitettu esimerkiksi lennokkiin tai tykistön tai raketinheitinten kantoammuksiin. Se voi olla myös käsin paikalle asetettava.

**Läpipolttoetäisyys** (burnthrough range) on etäisyys tutkasta, jota lähempänä olevan maalin tutka havaitsee häirinnästä huolimatta; tätä pidemmillä etäisyyksillä omasuojahäirintä on tehokasta, ja tutka ei havaitse maalia. Läpipolttoetäisyys riippuu mm. maalin tutkapoikkipinnasta, tutkan lähetystehosta ja häirintätehosta.

**Maalinosoitus** (target acquisition, TA) tarkoittaa vaikuttamisjärjestelmän tarvitsemien havaitun maalin ominaisuuksien, kuten sijainnin ja liikevektorin, määrittämistä vaikuttamisjärjestelmän edellyttämällä tarkkuudella ja vaikuttamistehtävän välittämistä vaikuttamisjärjestelmälle.

**Maalitus** (targeting) tarkoittaa prosessia, jossa valitaan mihin tiedustelu- ja valvontajärjestelmillä havaittuihin maaleihin vaikutetaan ja jossa maalit priorisoidaan sekä annetaan vaikuttamistehtävä jollekin vaikuttamisjärjestelmälle. Vaikuttamistehtävä käsittää maalin vaikuttamisjärjestelmän tai -menetelmän käskemisen, maalitietojen antamisen sekä halutun vaikutuksen käskemisen. Komentaja määrittää halutun vaikutuksen taisteluajatuksessaan.

**Mittaustiedustelu**, katso *elektroninen mittaustiedustelu*.

**Oikosulkuase** (short circuit weapon) on pommi tai ohjus, jonka hyötykuormana on ilmassa leviävää ja kohdejärjestelmissä oikosulkuja aiheuttavaa materiaalia, kuten hiilikuitusäikeitä tai hiilipölyä. Hiilikuitusäikeitä on käytetty jo Persianlahden sodassa 1991 sähkönjakeluverkon kytkinkenttien lamauttamiseen. Säikeet tarttuvat avojohtoihin ja –kytkimiin aiheuttaen niissä oikosulkuja. Hiilipölyä on suunniteltu käytettäväksi samassa tarkoituksessa: kevyt pöly ohjautuu ilman mukana tietokoneiden ja muiden elektronisten laitteiden tuuletinten kautta piirilevyille, missä aiheuttaa oikosulkuja. Sotilaselektroniikkaan pölyase ei vaikuta, mutta käytettävän kaupallisen elektroniikan toimintaa se kykenee häiritsemään.

**Operaatioturvallisuus** (operations security, OPSEC) käsittää operaation onnistumisen kannalta kriittisen informaation tunnistamisen, oman operaation kannalta keskeisen tiedon saatavuuden turvaamisen, arvion vastustajan tiedustelujärjestelmän kyvystä kerätä erilaista informaatiota, vastustajan valvonnan, arvion vastustajan keräämästä oman toimintamme kannalta kriittisestä informaatiosta, tiedusteltavuuden minimointiin tähtäävät keinot, tietovuotojen aiheuttamien kielteisten vaikutusten minimoinnin ja kriittisen tiedon fyysisen sijaintipaikan turvallisuuden (fyysinen turvallisuus).

**Operatiivinen harhauttaminen** (operational deception) on operatiivisella taholla tehtävää harhauttamista, jonka ensisijaisena kohteena on vastustajan pääjoukon komentaja. Komentajan tekemiin päätöksiin pyritään vaikuttamaan syöttämällä harhauttavaa tietoa vastustajan tiedonkeruukanaviin.

**Paikantamis- ja navigointisodankäynti** (navigation warfare, NAVWAR), käsittää pääosin elektronisen sodankäynnin keinoin toteutettavan paikantamisjärjestelmien häirinnän ja lamauttamisen sekä näiltä toimilta suojautumisen.

**Passiivinen elektroninen suojautuminen** (passive electronic protection) tarkoittaa järjestelmien suunnittelua ja käyttöä siten, että elektronista uhkaa erikseen havaitsematta haitataan tai estetään vastustajan suorittamaa tiedustelua, valvontaa, tai vaikuttamista.

**Psykologinen operaatio** (psychological operation, PSYOP) on psykologisen sodankäynnin keinoin suoritettava informaatio-operaatio tai sen osa. Psykologinen operaatio voi olla luonteeltaan hyökkäyksellinen tai puolustuksellinen – tai molempia.

**Radioelektroninen taistelu** (Radioelektronnaja borba, REB) on venäläisessä käsitemaailmassa esiintyvä termi, jolla tarkoitetaan länsimaita laajemmin elektronisen sodankäynnin komponenttien lisäksi myös fyysinen vaikuttaminen samoihin kohteisiin, sekä vahva harhautustoiminta. Anglo-amerikkalaisissa lähteissä REB on käännetty termiksi Radio Electronic Combat, REC.

**Radiohiljaisuus** (radio silence) tarkoittaa Suomessa sitä, että radiolaitteiden virta on katkaistu.

**Radiotaajuinen ase** (RF-ase, radio frequency weapon, RF Weapon) on ase, jonka vaikutus perustuu matala- (EMP-ase) tai korkeataajuisen (HPM-ase) sähkömagneettisen säteilyn tuottamiseen ja kohdentamiseen maalina olevaan järjestelmään, jonka elektroniikan toimintaa säteily häiritsee tai lamauttaa pysyvästi.

**Saattohäirintä** (escort jamming) on tukihäirinnän laji, jossa häirintäajoneuvo, -lentokone tai -alus liikkuu hyökkäävän osaston mukana ja suojaa sitä vastustajan valvonnalta ja asevaikutukselta.

**Signaalitiedustelu** (signals intelligence, SIGINT) on strategiseen tiedusteluun liittyvää vastustajan sähkömagneettisiin signaaleihin kohdistuvaa tiedustelua, jonka tarkoituksena on havaita vastustajan sähkömagneettisen spektrin käyttö, analysoida, luokitella ja tunnistaa vastustajan lähetteet sekä luokitella, tunnistaa, yksilöidä ja paikantaa vastustajan elektroniset järjestelmät ja assosioida havaitut lähetteet joukkoihin tai järjestelmiin. Signaalitiedustelun antamia tietoja käytetään yhtenä tiedustelulähteenä vihollistilannekuvan muodostamiseen, uhkavaroitukseen, omien vastatoimenpiteiden valmistelemiseen sekä omien hyökkäystoimenpiteiden vaikutuksen arvioimiseen. Signaalitiedustelusta ja elektronisesta tiedustelusta voidaan sen kohteen perusteella käyttää nimityksiä elektroniseen mittaustiedustelu ja elektroninen viestitiedustelu. Signaalitiedusteluun voidaan katsoa kuuluvaksi myös hajasäteilytiedustelu ja telemetriatiedustelu**.**

**Signaaliturvallisuus** (signal security) käsittää sekä viestiliikenneturvallisuuden että elektronisen turvallisuuden. (US joint EW doctrine)

**Sivukeilataso** (sidelobe level, SLL) on suure, joka kertoo kuinka paljon pienempi antennin vahvistus keskimäärin tai tietyissä sivukeiloissa on pääkeilaan nähden pääkeilan ulkopuolella. Keskimääräinen antennivahvistus pääkeilan ulkopuolella on siis antennin vahvistus (pääkeilan suuntaan) vähennettynä keskimääräisellä sivukeilatasolla.

**Sotamoodit** (wartime reserve modes, WARM) tarkoittavat sensori-, tiedonsiirto-, navigointi-, omatunnistus-, omasuoja-, ase- ja ELSO-järjestelmien teknisiä ominaisuuksia, jotka vaihdetaan sotatilanteessa erotukseksi rauhanaikaisessa harjoituskäytössä olleista ominaisuuksista. Tällä pyritään vaikeuttamaan vastustajan tiedustelua ja vastatoimien kehittämistä vähentämällä rauhanaikaisen tiedustelun merkitystä. Sotamoodien käyttöönoton myötä muutettavia parametreja ovat esimerkiksi keskitaajuus, kaistanleveys, salausalgoritmi ja taajuudenhypytysnopeus.

**Spektrinhallinta** (spectrum management) tarkoittaa spektrin käytön suunnittelua, ohjaamista ja valvontaa. Spektrin hallinta käsittää hallinnolliset, operatiiviset ja tekniset toimet ja keinot, joilla taataan spektrin käytön osalta sähkömagneettista spektriä käyttävien laitteiden ja järjestelmien toimivuus sekä joukon operatiivinen suorituskyky taistelukentällä. Spektrin hallintaan kuuluu elementtejä elektronisesta sodankäynnistä, taajuushallinta ja emissioiden hallinta.

**Suojatut taajuudet** (protected frequencies) ovat amerikkalaisen määritelmän mukaan omassa käytössä olevia taajuuksia, joiden käytettävyys on varmistettava. Näitä taajuuksia ei saa häiritä, ellei se ole operatiivisen toiminnan kannalta tarpeellista.

**Suunnatun energian ase** (directed-energy weapon, DEW) on ase, jonka toiminta perustuu suunnattuun energiavirtaan, kuten radiotaajuiseen tai optiseen säteilyyn tai suureen nopeuteen kiihdytettyihin hiukkasiin (hiukkasaseet). Ensin mainituista käytetään nimitystä radiotaajuiset aseet, optisen säteilyn aseista laseraseet.

**Suurtehomikroaaltoase** (high power microwave weapon, HPM Weapon) on mikroaaltoalueella, tyypillisesti 1-10 GHz taajuuksilla, toimiva suunnatun energian ase.

**Sähkömagneettinen yhteensopivuus** (electromagnetic compatibility, EMC) tarkoittaa järjestelmien, laitteiden ja moduulien kykyä toimia niille suunnitellussa käyttöympäristössä ilman niiden suorituskyvyn laskemista hyväksyttävän tason alapuolelle tai ilman että ne itse aiheuttavat muiden laitteiden suorituskyvyn laskemisen sähkömagneettisen säteilyn vuoksi. Sähkömagneettiseen yhteensopivuuteen kuuluu siten sekä kyky sietää sähkömagneettisia häiriöitä että riittävän pienet laitteesta lähtevät sähkömagneettiset häiriöt.

**Taajuushallinta** (frequence managemeng) käsittää taajuuksien käyttöön saamisen ja taajuuksien käyttöoikeuksien jakamisen ja käytön ohjeistuksen sekä taajuuksien käytön valvonnan. Taajuushallinta on *spektrinhallinnan* osa.

**Taajuuskonfliktien ratkaisu** (frequency deconfliction) on amerikkalaisen elektronisen sodankäynnin doktriinin mukaan systemaattinen prosessi, jolla taataan sähkömagneettisen spektrin käyttö omassa toiminnassa osana sähkömagneettisen spektrin käytön hallintaa.

**Taustahäirintä** (stand-off jamming) on tukihäirinnän laji, joka on operaatioalueella toimivaa häirintää, jolla tuetaan operaation suorittamista yleensä omien joukkojen selustassa tai omassa hallussa olevassa ilmatilassa. Taustahäirintä toteutetaan yleensä ilmasta, jolloin häirintäsignaalin vaimennus on pieni ja häirinnän kantama siten pitkä. Taustahäirinnän tavoitteena voi olla vastustajan sensoreiden häirintä siten, ettei se kykene havaitsemaan operaatioalueella toimivia joukkoja ja järjestelmiä, eikä operaation aikautusta tai suuntautumista.

**Telemetriatiedustelu** (telemetry intelligence, TELINT) tarkoittaa vastustajan järjestelmien ja laitteiden (esimerkiksi ohjukset) tutkimus-, kehitys- ja käyttövaiheisiin liittyvien mittaus- ja raportointilaitteiden lähetteiden sieppaamista ja analysointia.

**Tietojärjestelmäsodankäynti** (information system warfare, ISW, tai kapeammin ymmärrettynä tietoverkkosodankäynti net warfare, NW) on omien tietojärjestelmissä sijaitsevien tietojen, niitä käsittelevien tietojärjestelmien ja niiden käyttämän tiedonsiirron suojaamista sekä vaikuttamista vastustajan tietojärjestelmiin, tiedonsiirtoon ja niiden sisältämään tietoon. Tietojärjestelmäsodankäynti jakautuu 1) omien tietojärjestelmien valvontaan ja suojaamiseen ja 2) vastustajan tietojärjestelmiin kohdistuvaan tiedusteluun ja valvontaan sekä 3) tietojärjestelmähyökkäyksiin.

**Tietosodankäynti**: Termin sijasta puolustusvoimissa käytetään termiä informaatio-sodankäynti.

**Tukihäirintä** (support jamming) tarkoittaa häirintää, jossa häirintäjärjestelmä suojaa jotakin muuta järjestelmää. Tukihäirintä voidaan jakaa edelleen tausta-, saatto- ja lähi-häirintään sen mukaan miten häirintäjärjestelmä sijoittuu häirittävään kohteeseen ja häirinnällä suojattavaan kohteeseen nähden.

**Vaikutuspohjainen maalitus** (effects based targeting) tarkoittaa maalitusprosessia, jossa tarkastelun lähtökohtana on haluttu vaikutus vastustajan toimintaan. Halutun vaikutuksen perusteella määritetään kohde, johon vaikutetaan. Kohteen sekä käytettävissä olevien keinojen perusteella määritetään vaikuttamismenetelmä, joka voi olla myös mikä tahansa informaatiosodankäynnin osa-alueista.

**Valvotut taajuudet** (guarded frequencies) ovat vastustajan käytössä olevia taajuuksia, joita valvotaan elektronisen tuen järjestelmillä. Näitä taajuuksia voidaan myös häiritä, mikäli operatiivisen toiminnan kannalta on tärkeämpää estää vastustajaa käyttämästä niitä kuin itse hankkia tietoja vastustajan toiminnasta.

**Viestitiedustelu** katso *elektroninen viestitiedustelu*.

# LIITE 8: KÄYTETYT LYHENTEET

| | |
|---|---|
| AM | Amplitudimodulaatio |
| ARM | Anti-Radiation Missile, säteilyyn hakeutuva ohjus |
| AWACS | Airborne Warning And Control System, lentävä ennakkovaroitus- ja taistelunjohtojärjestelmä |
| BDA | Battle Damage Assessment, kohdevaikutuksen arviointi |
| C2 | Command and Control, johtaminen (käskytys ja valvonta/ohjaus) |
| C2W | Command and Control Warfare, johtamissodankäynti, JOSO |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance, tiedustelu, valvonta ja johtaminen (TVJ) |
| CAOC | Combined Air Operations Center |
| CDMA | Code Division Multiple Access, erilaisiin hajotuskoodeihin perustuva lähetteiden erottelumenetelmä |
| CIMIC | Civil – Military Co-operation, siviili- ja sotilastoimijoiden yhteistyö, yleensä kriisinhallintaoperaatiossa |
| COMINT | Communications Intelligence, viestitiedustelu |
| COMSEC | Communications Security, viestiliikenneturvallisuus |
| COTS | Commercial-Off-The-Shelf, kaupallisten tuotteiden hyväksikäyttö sotilasjärjestelmissä ja -operaatioissa |
| CW | Continuous Wave, jatkuvan aallon lähettämiseen perustuva (järjestelmä) |
| DEAD | Destruction of Enemy Air Defences, vastustajan ilmapuolustuksen tuhoaminen |
| DEW | Directed-Energy Weapon, suunnatun energian ase, joita ovat laseraseet ja hiukkasaseet sekä radiotaajuisista aseista HPM-ase |
| DIRCM | Directed IR Countermeasures, suunnattu (ohjusten hakupäiden ja infrapuna-maalinseurainten) infrapunahäirintä |
| DRFM | Digital Radio Frequency Memory, radiosignaalin suoran tallentamisen mahdollistava muisti, jota käytetään erityisesti tutkahäirintäsignaalien tallentamiseen ja toistamiseen |
| DS | Direct Secuency (Spread Spectrum), suorahajotus(hajaspektri-menetelmä), lyhennetty muoto lyhenteestä DSSS |
| DSSS | Direct Secuence Spread Spectrum, suorahajotushajaspektrimenetelmä |

| | |
|---|---|
| E3 | Electromagnetic Environmental Effects, sähkömagneettisen säteilyn ympäristövaikutukset |
| EA | Electronic Attack, elektroninen vaikuttaminen, ELVA |
| ECCM | Electronic Counter-Counter-Measures, vastatoimet elektronisille vastatoimille, vanha termi, joka tarkoittaa nykyisessä terminologiassa elektronista suojautumista |
| ECM | Electronic Counter-Measures, elektroniset vastatoimet, vanha termi, joka tarkoittaa nykyisessä terminologiassa elektronista vaikuttamista |
| EIRP | Equivalent Isotropic Radiated Power, teho, joka antennista lähtee pääkeilan suuntaan verrattuna isotrooppisesta säteilijästä joka suuntaan lähtevään tehoon. Yksikön käyttö helpottaa tehotasojen laskemista eri etäisyyksistä antennista. EIRP sisältää todellisen lähetystehon lisättynä antennin vahvistuksella (yleensä pääkeilan suuntaan). |
| ELSO | Elektroninen sodankäynti |
| ELSU | Elektroninen suojautuminen |
| ELTU | Elektroninen tuki |
| ELVA | Elektroninen vaikuttaminen |
| ELINT | Electronic Intelligence, elektroninen mittaustiedustelu |
| EMC | Electromagnetic Compatibility, sähkömagneettinen yhteensopivuus |
| EMCON | Emission Control, emissioiden hallinta: mitä järjestelmiä saa missäkin tilanteessa käyttää aktiivisena |
| EMI | Electromagnetic Interference, sähkömagneettiset (keskinäis)häiriöt |
| EMP | Electromagnetic Pulse, sähkömagneettinen pulssi |
| EMS | Electromagnetic Susceptibility, kyky sietää sähkömagneettista säteilyä |
| EMSEC | Emission Security, emissioturvallisuus |
| EOB | Electronic Order of Battle, elektroninen taistelujaotus |
| EP | Electronic Protection, elektroninen suojautuminen, ELSU |
| ERP | Effective Radiated Power, teho, joka antennista lähtee pääkeilan suuntaan verrattuna dipoliantennista lähtevään tehoon. ELSO-yhteyksissä suositellaan käytettäväksi käsitettä EIRP. |
| ES | Electronic Support, elektroninen tuki, ELTU |
| ESD | Electro-Static Discharge, staattisen sähkövarauksen purkautuminen |
| ESM | Electronic Support Measures, elektroninen tuki, vanha termi, joka tarkoittaa nykyisessä terminologiassa samaa kuin ES |
| EW | Electronic Warfare, elektroninen sodankäynti, ELSO |

| | |
|---|---|
| EWCC | Electronic Warfare Coordination Cell, elektronisen sodankäynnin koordinointisolu |
| FAPSI | Venäjän hallituksen viestiyhteys- ja informaatiopalvelu (siviilisignaalitiedustelu) |
| FH | Frequency Hopping, taajuushypintäjärjestelmä |
| FM | Frequency Modulation, taajuusmodulaatio |
| GENFORCE | Generic Enemy Force, brittien geneerinen harjoitusvastustaja |
| GHz | Gigahertsi, miljardi hertsiä |
| GMTI | Ground Moving Target Indication, liikkuvien maamaalien ilmaisu(tutka) |
| GRU | Venäjän asevoimien tiedustelupäähallinto |
| GPS | Global Positioning System, maailmanlaajuinen satelliittipaikannusjärjestelmä. Nimitys on sekä yleisnimitys globaalille satelliittipaikannukselle, että erisnimi amerikkalaiselle NAVSTAR-satelliitteihin perustuvalle paikannusjärjestelmälle. Mikäli käsitettä GPS käytetään yleisnimityksenä, siihen kuuluvat nykyisin amerikkalaisen GPS-järjestelmän lisäksi venäläinen GLONASS ja tuleva yhteiseurooppalainen Galileo. |
| HERO | Hazards of EM Radiation to Ordnance, sähkömagneettinen säteilyn aikaansaama räjähteiden, ammusten, taistelukärkien ja rakettimoottoreiden virhetoimintariski |
| HF | High Frequency, taajuusalue 3-30 MHz |
| HPM | High-Power Microwave, suuritehoinen mikroaaltosäteily(ase) |
| IA | Information Attack, informaatiohyökkäys |
| IFF | Identification Friend or Fore, omatunnistusjärjestelmä |
| INS | Inertial Navigation System, inertianavigointijärjestelmä |
| IO | Information operation, informaatio-operaatio |
| IOCC | Information Operation Coordination Cell, informaatio-operaation koordinointisolu |
| IP | Infrapuna, aallonpituusalue 780 nm – 1 mm |
| IRP | Interference Reference Point, interferenssinilmoituspiste |
| IS | Information Superiority, informaatioylivoima |
| ISAR | Inverse Synthetic Aperture Radar; esim. merivalvontakoneissa käytetty tutkamoodi, jolla voidaan tunnistaa havaittuja kohteita. |
| ISTAR | Intelligence, Surveillance, Target Acquisition and Reconnaissance, tiedustelu, valvonta ja maalinosoitus. Myös muotoa IRSTA käytetään. |

| | |
|---|---|
| ISR | Intelligence, Surveillance and Reconnaissance, tiedustelu ja valvonta |
| ISW | Information System Warfare, tietojärjestelmäsodankäynti |
| IW | Information Warfare, Informaatiosodankäynti |
| J2 | Tiedusteluala puolustushaarojen yhteisessä (joint) NATO-esikunnassa |
| J3 | Operatiivinen ala puolustushaarojen yhteisessä (joint) NATO-esikunnassa |
| J5 | Suunnitteluala puolustushaarojen yhteisessä (joint) NATO-esikunnassa |
| J6 | Viesti/johtamisjärjestelmäala puolustushaarojen yhteisessä (joint) NATO-esikunnassa |
| JCA | Jamming Control Authority, häirinnänohjausviranomainen |
| JOSO | Johtamissodankäynti (engl. C2W) |
| JRFL | Joint Restricted Frequency List, kiellettyjen taajuuksien lista |
| JSR | Jamming to Signal Ratio, häirintäsignaalin suhde hyötysignaaliin (katso myös SJR) |
| JSTARS | Joint Surveillance And Target Acquisition Radar System, Yhdysvaltain puolustusvoimien ilma- ja maavoimien yhteiskäyttöinen lentävä tiedustelu- ja valvonta- sekä maalinosoitusjärjestelmä maakohteita vastaan. |
| kHz | Kilohertsi, tuhat hertsiä |
| LPD | Low Probability of Detection, järjestelmä, jonka signaali on vaikeasti ilmaistavissa |
| LPE | Low Probability of Exploitation, järjestelmä, jonka signaali on vaikeasti hyödynnettävissä |
| LPI | Low Probability of Intercept, järjestelmä, jonka signaali on vaikeasti siepattavissa |
| µm | mikrometri |
| MHz | Megahertsi, miljoona hertsiä |
| MIJI | Meaconing (paikantamis- ja navigointijärjestelmien häirintä ja harhauttaminen), Intrusion (tunkeutuminen viestiverkkoon), Jamming (tahallinen häirintä), Interference (tahattomat häiriöt) |
| MIMO | Multiple Input – Multiple Output, eräs uusi signaalien prosessointitapa |
| MSTO | Minimum Safe to Operate, vähimmäisvaatimukset, joiden täyttäminen on edellytys turvalliselle osallistumiselle operaatioon |
| MTI | Moving Target Indicator; liikkuvan maalin ilmaisu tutkajärjestelmässä |
| NACSI | NATO:n SIGINT-committee |
| NAVWAR | Navigation Warfare, paikantamissodankäynti |

| | |
|---|---|
| NBC | Nuclear, Biological, Chemical, joukkotuhoaseet |
| NBF | Net-Baserad Försvar, verkkokeskeinen puolustus |
| NCW | Network-Centric Warfare, verkostokeskeinen sodankäynti |
| NEC | Network-Enabled Capability, verkon mahdollistama suorituskyky (harvoin käytetty lyhenne) |
| NEDB | NATO Emitter Database, NATO:n jäsenilleen jakama uhkaparametritietokanta |
| NEWAC | NATO EW Advisory Committee |
| nm | nanometri |
| NW | Net Warfare, tietoverkkosodankäynti |
| OODA | Observe – Orientate – Decide – Act |
| OPFOR | Opposing Force, amerikkalaisten geneerinen harjoitusvastustaja |
| OPSEC | Operations Security, operaatioturvallisuus |
| PA | Public Affairs, PR-toiminta |
| PGM | Precision-Guided Weapon, täsmäase |
| PI | Public Information, tiedottaminen |
| POD | Probability of Detection, (signaalin) ilmaisun todennäköisyys |
| POE | Probability of Exploitation, todennäköisyys, jolla signaali voidaan hyödyntää tiedustelussa |
| POI | Probability of Intercept, (signaalin) sieppaustodennäköisyys |
| PSYOP | Psychological Operation, psykologinen operaatio |
| REB | Radioelektronnaja borba, radioelektroninen taistelu – venäläinen nimitys elektroniselle sodankäynnille |
| RF | Radio Frequency, radiotaajuus. Taajuusalue, jolla signaali voi edetä sähkömagneettisena säteilynä. |
| RFGM | Radio-Frequency Guided Munition, radiotaajuiseen säteilyyn hakeutuva ammus |
| RFI | Request for Information, tietopyyntö yritykselle hankintaprojektin tiedonhankintavaiheessa |
| RFQ | Request for Quotation, tarjouspyyntö |
| ROE | Rules of Engagement, voimankäytön säännökset, suomeksi VOKS |
| SA | Situational Awareness, tilannetietoisuus |
| SAR | Synhtetic Aperture Radar, synteettisen apertuurin tutka |
| SATCOM | Satellite Communication, satelliittitietoliikenne |

| | |
|---|---|
| SEAD | Suppression of Enemy Air Defences, vastustajan ilmapuolustuksen lamauttaminen |
| SC | (NATO) Strategic Command |
| SHF | Super-High Frequency, taajuusalue 3-30 GHz |
| SIGINT | Signals Intelligence, strategiseen tiedusteluun kuuluva signaalitiedustelu |
| SJNR | Signal-to-Jamming&Noise Ratio, hyötysignaalin suhde häirintäsignaalin ja kohinatason summaan |
| SJR | Signal-to-Jamming Ratio, hyöty/häirintä-signaalisuhde (katso myös JSR) |
| SLAR | Sideways-Looking Airborne Radar, sivuviistotutka |
| TA | Target Acquisition, maalinosoitus |
| TALD | Tactical Air-Launched Decoy, ilma-aluksesta pudotettava vapaasti lentävä harhaliidokki tai matkamoottorilla varustettu harhamaali |
| TELINT | Telemetry Intelligence, telemetriatiedustelu |
| TPA | Tehtävät ja toiminnan perusajatus |
| TVJ | Tiedustelu, valvonta ja johtaminen, englanniksi C4ISR |
| UAV | Unmanned Aerial Vehicle, miehittämätön ilma-alus eli lennokki |
| UHF | Ultra-High Frequency, taajuusalue 300 MHz – 3 GHz |
| USV | Unmanned Surface Vehicle, miehittämätön pinta-alus |
| UV | Ultravioletti, aallonpituusalue 100 – 400 nm |
| VHF | Very High Frequency, taajuusalue 30-300 MHz |
| VOKS | VOimanKäytön Säännökset, ROE, Rules of Engagement |
| WARM | Wartime Reserve Mode(s), sotamoodit eli toimintaparametrijoukko, joka otetaan käyttöön vasta kriisitilanteessa. Tällä estetään vastustajia optimoimasta tiedustelu- ja häirintäjärjestelmiään järjestelmien rauhanaikaisen tiedustelun tuottamien tietojen perusteella. |

# LIITE 9: LÄHDEVIITTEET JA HUOMAUTUKSET

[1] Esimerkiksi NATO:n maavoimien sodankäyntikyvyn kehittämisen avainteknologioiksi mainitaan mm. elektronisen sodankäynnin, informaatiosodankäynnin ja suunnatun energian aseiden teknologiat. Land Operations in the Year 2020, NATO RTO Technical Report 8. Maaliskuu 1999.

[2] Juri Klenov: Rasskazivajem vpervie. Sankt-Peterburgskie Vedomosti No 38 (2428) 28.2.2001 http://www.pressa.spb.ru/newspapers/spbved/2001/arts/spbved-2428-art-6.html. Haettu 6.8.2004. Lisää venäläisestä elektronisesta sodankäynnistä on luettavissa osoitteesta http://www.reb100.mil.ru, joka on Venäjän Puolustusministeriön ELSO:n satavuotissivusto.

3 Jyri Kosola ja Tero Solante: Digitaalinen taistelukenttä – informaatioajan sotakoneen tekniikka. Toinen, korjattu ja laajennettu painos. Maanpuolustuskorkeakoulun Tekniikan Laitoksen julkaisusarja 1, julkaisu 13/2003. ISBN 951-25-1449-4. 532 s. Oppikirja elektronisten tiedustelu-, valvonta-, johtamis- ja asejärjestelmien tekniikasta ja hyödyntämisestä nykyaikaisella taistelukentällä.

[4] Ali Mättölä: Liikkuvien voimien armeijakunnan rooli Venäjän sotataidon kehittymisessä 2000-luvun alkupuolella. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisusarja 1, numero 2/1998. s. 18.

[5] Vaikka verkkokeskeisen sodankäynnin käsite onkin otettu käyttöön korostamaan 2005-2025 käyttöön tulevien uusien (korkeateknologisten) järjestelmien lähes täydellistä riippuvuutta verkostoista, pätee tämä riippuvuus moniin jo nykyisinkin käytössä oleviin järjestelmiin. Esimerkkinä käy epäsuoran tulen järjestelmä tai vaikkapa yhteisiin tiedustelujärjestelmiin, keskitettyyn johtamiseen ja kaukovaikutteiseen tulenkäyttöön perustuvat järjestelyt, kuten Venäjän maa-, meri- ja ilmavoimien toiminta. Ensin mainitusta hyvänä kuvauksena käy lähde Ali Mättölä: *Venäjän asevoimien yleiset kehitysnäkymät* (s. 49) ja toisesta Harri Tielinen: *Venäjän merivoimien suorituskyky ja maihinnousuoperaatioiden kehitysnäkymät Itämeren alueella* (s. 73) ja viimeksi mainitusta Heikki Nikunen: *Venäjän ilmavoimien nykytila* (s. 92-93). Edellä mainitut lähteet Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisussa *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9.

[6] Joissakin yhteyksissä näkee käytettävän nimityksiä elektromagneettinen säteily ja elektromagneettinen spektri, jotka on suomennettu väärin englanninkielen sanoista electromagnetic radiation ja electromagnetic spectrum. Suomeksi electromagnetic = sähkö-magneettinen (vertaa sähkövirta eikä elektrovirta).

[7] Esimerkiksi venäläisen näkemyksen mukaan taistelun voittaminen sähkömagneettisessa spektrissä merkitsee tulevaisuudessa koko taistelun voittamista. Jorma Saarelainen: *Informaatiosodankäynti – venäläinen näkökulma*. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 258-259.

[8] Suomessa termi Electronic Attack, siis elektroninen hyökkäys, on käännetty paremmin suomalaiseen yhteiskuntaan sopivaan muotoon elektroninen vaikuttaminen, sillä elektronista vaikuttamista voidaan käyttää myös puolustus- ja suojaamismielessä.

[9] Muita keskeisiä säteilyä kuvaavia suureita ovat aallonpituus, teho, energia ja polariteetti. Säteilyn aallonpituus kuvaa yhden värähtelyjakson pituuden aallon edetessä ja sen yksikkö on metri [m]. Aallolla on tietty teho (watti [W]) tai tehotiheys (wattia taajuus- tai pinta-alayksikköä kohti, W/Hz tai $W/m^2$). Lähetetty, siirretty tai vastaanotettu teho jonakin aikana muodostaa lähetetyn, siirretyn tai vastaanotetun energian (energia = teho · aika). Säteilyn polariteetti puolestaan kertoo missä suunnassa säteilyn sähkökenttä värähtelee.

[10] Sähkömagneettisesta yhteensopivuudesta käytetään usein suomessakin nimitystä EMC sen englanninkielisen nimityksen Electromagnetic Compatibility vuoksi. Sähkömagneettisella yhteensopivuudella tarkoitetaan laitteiden tai järjestelmien kykyä toimia sähkömagneettisessa toimintaympäristössä ilman että niiden toimintakyky heikkenee olennaisesti tai lakkaa kokonaan. Sähkömagneettinen yhteensopivuus sisältää sekä kyvyn sietää ympäristössä olevaa sähkömagneettista säteilyä (EMS, Electromagnetic Susceptibility) että oman muita laitteita häiritsevän säteilyn rajoittamisen (EMI, Electromagnetic Interference).

[11] Sähkömagneettinen säteily voi saada aikaan räjähteiden, ammusten, taistelukärkien ja rakettimoottoreiden virhetoiminnan. Tätä kutsutaan nimellä HERO (Hazards of EM Radiation to Ordnance).

[12] Elektroniset laitteet, etenkin laitteet, jotka sisältävät MOS-tekniikalla toteutettuja puolijohteita (suurin osa digitaalisista mikropiireistä), ovat hyvin herkkiä staattisen sähkön purkauksille (ESD, Electro-Static Discharge).

[13] Michal Fiszer: *Red Fighters Revised*, The Journal of Electronic Defense, elokuu 2004, s. 44: Kun MiG-29:n ensimmäiset tuotantoversiot (9.12) otettiin käyttöön, koneeseen ei kuulunut siihen suunniteltu L-203BE Gardenia –häirintäjärjestelmä, koska se häiritsi liikaa lentokoneen avioniikkaa. Omasuojajärjestelmä saatiin lopulta integroitua kymmenisen vuoden viipeellä.

[14] Ted McKenna: *Hearing Impaired, The Journal of Electronic Defense*, elokuu 2004, ss. 36-41.

[15] NATO:ssa ELSO on määritelty samaan tapaan kuin Suomessa, eli sähkömagneettisen spektrin kautta tapahtuvaksi toiminnaksi. NATO:n ELSO-määritelmä sisältää kuitenkin myös hiukkasaseet sekä tutkahakuiset ohjukset. NATO:n määritelmässä on siten sisäisiä ristiriitaisuuksia.

[16] OODA-silmukan keksijänä pidetään amerikkalaista ilmavoimien everstiluutnanttia John Boydia. Lisää hänen ajatuksistaan voi lukea Grant T Hammondin kirjasta *The Mind of War. John Boyd and American security*.

[17] Kaarle Lagerstam, Juha-Antero Puistola, Torsti Siren: Yhdysvaltalainen sotilasstrategia tänään. Maanpuolustuskorkeakoulun Strategian laitoksen julkaisu: Julkaisusarja 2. Numero 21/2003. ISBN951-25-1444-3. s 40.

[18] Amerikkalaisen näkemyksen mukaan informaatiosodankäynnin eri osa-alueiden optimaalinen hyödyntäminen edellyttää kineettisten ja epäkineettisten aseiden maalitusprosessin yhdistämistä. Kineettisellä tarkoitetaan perinteistä fyysistä asevaikutusta, jossa ammutaan kineettisiä projektiileja. Epäkineettisellä tarkoitetaan vastaavasti kaikkia muita vaikutuskeinoja, kuten elektronista ja psykologista vaikuttamista. Zachary P. Hubbard: *IO in the information age*. Journal of the Electronic Defense. Toukokuu 2004. s. 52.

[19] Hyvänä esimerkkinä seurannaisvaikutusten arvioinnista toimii buurien päätös jättää lamauttamatta brittien johtamisyhteydet buurisodassa 1899–1902. Buurit arvioivat kykenevänsä katkaisemaan brittien lennättimeen perustuvat johtamisyhteydet ja siten vaikeuttamaan joukkojen siirtoja. Britit kykenisivät kuitenkin ennen pitkää korvaamaan lennätinyhteydet muilla menetelmillä ja osaisivat sopeuttaa toimintansa tähän. Buurit arvioivat tärkeämmäksi brittien viestiliikenteen kuuntelun, millä saatiin ennakkotietoja hyökkääjän toiminnan tarkoituksista, suuntautumisesta ja ajoituksesta.

[20] USA:n puolustustutkimuslaitos DARPA on saanut 2003 rahoituksen säteilyyn hakeutuvien krh-ammusten (RFGM, Radio-Frequency Guided Munition) kehittämiseksi. Ohjelma tunnetaan myös nimellä Destructive Suppression of Enemy Telecommunications - DeSERT. Ohjelman tavoitteena on saavuttaa vuonna 2007 teknologiademonstraattori, jossa modifioitu 81 mm kranaatinheittimen ammus kykenee vastaanottamaan ja prosessoimaan 30 MHz – 3 GHz signaaleja, paikantaa niiden lähteen viidessä sekunnissa ja hakeutuu 50-90% todennäköisyydellä 20 metriä lähemmäs maalia, jossa se räjähtää 3 metrin korkeudessa. Ammukseen syötetään ennen laukaisua kohdelähettimen kantoaallon taajuus, kaistanleveys ja modulaatio. Maalin paikka on tunnettava 1,5 km säteellä. Teknologiaa kaavaillaan käytettäväksi myös tykistön kranaateissa sekä pst- ja ilmasta-pintaan-ohjuksissa ja jopa olalta laukaistavissa ilmatorjuntaohjuksissa. *Radio frequency-guided mortar round to defeat communications/ electronic-warfare emitters*. Jane's International Defense Review. Maaliskuu 2004. s. 8.

[21] Harri Ohra-Aho: *Venäläinen näkemys sodan kuvasta*. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 44.

[22] Esimerkiksi venäläisellä tulenjohtajalla on oltava suora radioyhteys tulikomennon toteuttavaan tuliportaaseen. Tulenkäytön yhteydet perustuvat radioiden käyttöön: vain tulipatterin sisällä voidaan käyttää lisäksi johdinyhteyksiä. Sakari Wallinmaa: *Venäjän tykistön ja raketinheittimistön kehitysnäkymät*. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 107-108.

[23] Ali Mättölä: *Venäjän maavoimien yleiset kehitysnäkymät.* Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 48.

[24] Sakari Wallinmaa: *Venäjän tykistön ja raketinheittimistön kehitysnäkymät.* Maanpuolustus-korkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 118.

[25] USA:lla on (2003) kolme Commando Solo –konetta, jotka kykenevät lähettämään propagandaa AM-, FM-, lyhytaalto- ja TV-kaistoilla. Commando Solon lisäksi USAF on käyttänyt Compass Call -häirintälentokoneita paitsi sotatoimiensa tukemiseen, myös strategisen propagandan levittämiseen osana psykologista operaatiota. Kuuban kansaan ja hallitukseen vaikuttamiseksi vuonna 2003 lähetetyt ohjelmat sisälsivät sekä USAssa toimivan Kuubaan lähettävän TV-aseman lähetyksiä että USA:n presidentin kuubalaisille osoitetun puheen. Kenneth B. Sherman: *USAF Employs EW Aircraft Against Cuba*. The Journal of Electronic Defence. Heinäkuu 2003. s. 19.

[26] Kehitteillä ja osin palveluskäytössä olevat valokuituohjatut aseet kykenevät lähettämään lentoreitiltään videokuvaa näkyvän valon ja/tai infrapuna-alueelta. Kuva välitetään valokuitulinkkiä pitkin ohjuksen hakupäästä sen ampuneelle lavetille, josta se on lähetettävissä edelleen viestiverkossa esimerkiksi tiedustelukomppanian komentopaikalle.

[27] Michal Fiszerin ja Jerzy Gruszczynskin artikkelissa *Kolchugas Aid Saddam's Escape* esitetään, että Ukrainan Irakille myymä Kolchuga–ESM/ELINT-järjestelmä mahdollisti Saddan Husseinin paon amerikkalaisten ensi-iskusta antamalla muutamien minuuttien ennakkovaroituksen tulevasta F-117A-häivehävittäjähyökkäyksestä. Tämä on tietysti mahdollista, mutta silloin amerikkalaiset ovat käyttäneet ilma-asettaan väärin, koska jotta ELTU/ELINT kykenisi havaitsemaan F-117:n, on tämän lähetettävä jotakin sähkömagneettiseen spektriin. Tuolloin taas menetetään se etu, jonka häivetekniikka tuo. The Journal of Electronic Defence. Heinäkuu 2003. s. 28.

[28] Esimerkiksi saksalainen MRCM on julkaissut vuonna 2004 uuden kannettavien ES-laitteiden perheen. Sen vastaanotin kykenee havaitsemaan ja suuntimaan 2 MHz – 3,5 GHz taajuusalueella olevat lähetteet, eli käytännössä kaikki kenttäradiot, matkapuhelimet, viranomaisverkon radiopuhelimet ja johtamispaikkojen taktiset radiolinkit. *Lightweight ESM and DF Units*. The Journal of Electronic Defense. Elokuu 2004. s. 29.

[29] Andrew Koch: *Information warfare tools rolled out in Iraq*. Jane's Defence Weekly 6.8.2003. s. 7.

[30] NATO:n jalkaväkiaseiden kehitystä tarkastelevan suunnitelman luonnoksen mukaan ajoneuvo- tai alusasenteisen HPM-aseen teholliseksi kantamaksi arvioidaan kymmenisen kilometriä. Pommiin tai taistelulennokkiin asennetun aseen kantamaksi muutamaa kilometriä ja tykistö- tai kranaatinheitinten ammuksiin sovitetun HPM-kranaatin kantamaksi kymmeniä metrejä. *NATO infantry weapons master plan Draft 19.12.2003. s.* 3.

[31] Emissiolla tarkoitetaan kappaleen lähettämää säteilyä erotuksena kappaleesta heijastuvasta säteilystä. Kappaleet lähettävät toiminnallista säteilyä esimerkiksi tutka-, radio- tai lasersignaalin muodossa, elektronisten piirien ja sähkölaitteiden aikaan saamaa tahatonta säteilyä, jota kutsutaan hajasäteilyksi, sekä ns. mustan kappaleen (lämpö)säteilyä, joka on suurimmillaan infrapuna-aallonpituuksilla.

[32] Clark, John S. (USAF): *Joint EW reprogramming maintains a combat edge*. Journal of Electronic Defense, Military Microwave Supplement, elokuu 2004, ss. 24-32. Eversti Clarkin kirjoituksessa mainitaan, että Yhdysvaltain elektronisen sodankäynnin järjestelmät saadaan ohjelmoitua uudelleen tunneissa siitä kun uhkan muuttuminen on havaittu riippumatta siitä missä muutos on tapahtunut ja riippumatta siitä, missä uudelleen parametroitava järjestelmä sijaitsee.

[33] Teknologian kehittyminen mahdollistaa myös elektronisen tuen ja elektronisen häirinnän ominaisuuksien integroimisen osaksi viestivälineitä. Nick Cook: *Cause and Effect*, Jane's Defense Weekly 18.6.2003.

[34] Hyvän vaikuttavuuden vuoksi esimerkiksi Venäjällä on yleisessä käytössä ainakin 122 mm ja 152 mm tykistölle häirintäkranaatteja, joiden VHF- tai HF-häirintä kestää tunnista kahteen. Sakari Wallinmaa: *Venäjän tykistön ja raketinheittimistön kehitysnäkymät*. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999. ISBN 951-25-1102-9. s 115. Alkuperäinen lähde Jane's Ammunition Handbook 1994-1995. s. 461.

[35] Bill Sweetman: *Gripen – Lion of the Sky*. The Journal of Electronic Defense. Elokuu 2004, ss. 62-63.

[36] Amerikkalaisten mukaan F-15 hävittäjien varustaminen JTIDS-datalinkillä, joka mahdollisti lavettien välisen tiedonvaihdon sekä reaaliaikaisen tilannekuvan siirtämisen hävittäjille, nosti todellista taistelutilannetta jäljittelevissä harjoituksissa voitto/tappiosuhdetta arvosta 3:1 arvoon 8:1.William B.Scott: *Nascent Net-Centric War Gains Pentagon Toehold*. Aviation Week &Space Technology, 27.1.2003, s. 50.

[37] John A Tirpak: *Next Steps in Electronic Attack*. Air Force Magazine – Journal of the Air Force Association, kesäkuu 2002, vol 85 numero 6.

[38] Lähteen http://home/wanadoo.nl/tcc/balkan/allfor_forces.html (haettu Internetistä 9.9.2004) mukaan NATO menetti kaksi konetta taistelutehtävissä, mutta näistä vain yksi, F-117 menetettiin serbien SA-6-ohjustuleen toisen koneen (F-16CG) saadessa moottorihäiriön. Lähteen mukaan serbit onnistuivat ampumaan alas kolme amerikkalaista ja kolme saksalaista lennokkia. Eri lähteissä esiintyvät määrät ovat keskenään ristiriitaisia, mutta kokonaiskuva on yhdenmukainen: ELSO- ja SEAD/DEAD-koneiden käytöllä liittouma piti lentokonetappionsa käytännössä olemattomina, mutta ELSO:lla suojaamattomia lennokeita pudotettiin lukuisia.

[39] Jan-Olof Gran: *Signalspanarna får viktiga roller på det elektroniska slagfältet.* FOA Tidningen, nro 1, maaliskuu 1999.

[40] Pääesikunnan johtamisjärjestelmäosaston hallinnollinen ohje PAK 16:1: *Puolustusvoimien radiohallinto* 1.6.2001 puolustusvoimien esikuntajärjestelmän tietokannassa. Ohjeistus rajautuu radiotaajuuskaistalle, kuten sen perustana oleva radiolakikin, eli alle 3 THz taajuuksille. Optiselle taajuuskaistalle ei ole määritelty ohjeistusta.

[41] Esimerkiksi HMS Sheffieldin tuhoutuminen argentiinalaisten ampumiin Excocet-ohjuksiin johtui pitkälti siitä, että aluksen käyttämän SATCOM-järjestelmän käyttämä taajuus tukki laivan ELTU-järjestelmän vastaanottimen toiminnan hetkellä, jona elektroninen tuki olisi muutoin kyennyt varoittamaan tulossa olevasta ohjuksesta.

[42] Majuri Jouko Seitakarin esitysmateriaalista koostettu lyhyt kuvaus Puolustusvoimien taajuushallinnasta. Tarkempi ja laajempi kuvaus löytyy Pääesikunnan Johtamisjärjestelmäosaston pysyväisasiakirjoista.

[43] Yhdysvaltain puolustusministeriö julkaisi vuonna 2003 strategisen suunnitelman, jonka tavoitteena on kehittää spektrin hallintaa (spectrum management and electromagnetic environmental effects) osana business-prosesseja. Tähän liittyen ensi vaiheessa järjestelmävaatimuksissa otetaan huomioon myös niiden tarvitsema spektri ja jatkossa ryhdytään laatimaan järjestelmäarkkitehtuuria spektrinkäyttö huomioon ottaen. Kaikkien tulevien hankkeiden on hyödynnettävä spektriä tehokkaasti käyttäviä teknologioita ja tekniikoita. Kehittämissuunnitelman ytimenä on laatia kattava spektrinkäyttösuunnitelma, joka sisältää sekä asevoimien nykyisen spektrin käytön että suunnitellut tulevaisuuden tarpeet. Suunnitelma kuvaa myös asevoimien suorituskykyyn syntyvät rajoitukset ja haavoittuvuudet, mikäli spektrin tietyt osat eivät ole asevoimien käytettävissä. *Managing Defense Spectrum*, Signal. Helmikuu 2003. s. 6.

[44] Amerikkalaiset luopuivat F-4G Wild Weasel ja EF-111 Raven -saattohäirintä- ja SEAD-koneistaan ilmeisesti kaluston vanhenemisen lisäksi myös siitä syystä, että häiveteknologian katsottiin poistavan elektronisen häirinnän tarpeen ilmaoperaatioissa. Kuitenkin serbejä vastaan 1999 käydyssä sodassa pommitussuorituksia jouduttiin viivästämään ja perumaan häirintäkoneiden puuttumisen vuoksi, sillä ainut käytössä ollut saattohäirintäkykyinen kone oli laivaston EA-6B Prowler. Tästä ja Irakista saatujen kokemusten perusteella ryhdyttiin kehittämään F/A-18-koneesta uutta SEAD/DEAD/EA-versiota F/A-18 Growler:ia. John A Tirpak: *Next Steps in Electronic Attack.* Air Force Magazine – Journal of the Air Force Association, kesäkuu 2002, vol 85 numero 6.

[45] Viestijärjestelmien suojaaminen käsittää kaikki keinot, joilla estetään luvaton tiedon hankkiminen tai joilla tiedustelua johdetaan harhaan. US Joint Publication 3-51: Joint Doctrine for Electronic Warfare: GL 4.

[46] *Radio frequency-guided mortar round to defeat communications/electronic-warfare emitters*. Jane's Defense Review. Maaliskuu 2004, p. 8.

[47] Glenn W. Goodmann Jr.: *Improving Eavesdropping – U.S. SIGINT Aircraft Set Integrated Upgrade Paths.* Defense News 22.9.2003. s 24.

[48] Amerikkalaisten tavoitteena on kehittää 30 MHz – 3 GHz taajuuskaistalla toimiva päällepuettava ELTU-järjestelmä, joka varoittaa uhkan olemassaolosta ja antaa suunnan uhkalähettimeen. Näin laaja taajuusalue kattaa HF-, VHF- ja UHF-alueiden kenttäradiot, ilma- ja merivoimien radiot, matkapuhelimet ja osan kenttäteleverkkojen radiolinkeistä. *Body-worn DF for special forces.* Jane's International Defense Review. Heinäkuu 2004. s. 12.

[49] Amerikkalaiset ovat kehittämässä ilmasta tai maasta levitettäviä elektronisia paikantamis- ja häirintäjärjestelmiä. Järjestelmä muodostuu 6" x 4" kokoisista ja 6 paunaa painavista sylintereistä, jotka laskeuduttuaan maahan nostavat itsensä pystyyn ja nostavat puhallettavan antennin. Osa sylintereistä muodostaa verkon radioteitse ja paikantaa vastustajan komentokeskukset, joiden tietoliikenteen ne lamauttavat *WolfPack Attacks Enemy Lines: Signal, lokakuu 2003*. s. 8.

[50] Esimerkiksi yhä käytössä olevien tutkataajuuskaistojen nimet määritettiin siten, ettei niistä voi päätellä millä taajuusalueella laite toimii. Britit halusivat näin suojella omaa elektronisen sodankäynnin kykyään siltä varalta, että saksalaisten tiedustelu onnistuisi sieppaamaan sanomia joissa olisi viitattu taajuuskaistoihin niiden nimillä.

[51] Pääesikunnan Operatiivisen osaston asiakirja 2/11.2/D/I/19.01.2004 – *Strateginen suunnittelu puolustusvoimissa normaaliaikana*.

[52] Pääesikunnan Operatiivisen osaston ohje 18.6.2004: *Vaatimukset ja niiden hallinta puolustusvoimissa*.

[53] Pasivirta, Pasi ja Kosola, Jyri: *Vaatimustenhallinnan soveltaminen Puolustusvoimissa*. Edita Prima Oy 2004. ISBN 951-25-1548-2. 159 s.

[54] Martin Stephen: *Sea-Battles in close-up: World War 2*. Ian Allan ltd 1988. ISBN 0-71110-1596-1. ss. 175-177.

[55] Martin Stephen: *Sea-Battles in close-up: World War 2*. Ian Allan ltd 1988. ISBN 0-71110-1596-1. ss. 202-217.

[56] Victor. A. Pheasant: *Window on Gomorrah*. The Journal of Electronic Defense, heinäkuu 2003. ss 56-59.

[57] R. V. Jones: *Most Secret War*. Wordsworth Edition Limited 1998, ISBN 1-85326-699, ss. 215-222.

[58] Kokoavan näkemyksen on esittänyt elektronisen sodankäynnin asiantuntija ja tutkija evl evp Sakari Ahvenainen.

[59] Tshetshenia-kappale on pääosin referaatti eversti Jari Kähärän tekemästä koonnoksesta asiaa käsittelevistä venäläisistä julkisista lähteistä. Aiheesta kiinnostunut lukija löytää paljon lisätietoa mm. Internetistä.

[60] Tshetshenian opetuksia on mielenkiintoista verrata Venäjän samojen aikojen suunnitelmiin oman järjestelmänsä kehittämiseksi, joiden mukaan uusia ELSO- ja viestijärjestelmiä ja -joukkoja on aiottu ottaa käyttöön. Ks. esim. Juha Wihersaari: *Venäjän viesti- ja elso-järjestelmien kehitysnäkymät*. Maanpuolustuskorkeakoulun Taktiikan Laitoksen julkaisu *Venäjän asevoimat 2000-luvun alussa*. Julkaisusarja 2, numero 1/1999.

[61] Venäjän julkistetun vuoden 2003 puolustusbudjetin merkittävin osa-alue on elektroninen sodankäynti: ELSO 29,2 mrd ruplaa, laivaston alukset 16,8 mrd, lentokoneet 11,0 mrd, panssaroidut ajoneuvot 5,3 mrd, a-tarvikkeet 4,8 mrd, tykistöaseet 1,8 mrd ja käsiaseet 1,0 mrd. DefenseNews 20.10.2003. s. 13.

[62] Douglas A. Macgregor: *Breaking the Phalanx, a New Design for Landpower in the 21st Century*. Praeger Publishers 1997, ISBN 0-275-95793-4. s. 32.

[63] Yhdysvaltain puolustusministeriön julkaisu *Joint Operations Concepts*, marraskuulta 2003 korostaa tekniikan, organisaation ja doktriinin yhdenmukaisen ja samanaikaisen kehittämisen merkitystä sotilaallisen suorituskyvyn luomisessa.

[64] Eversti Mark Gunziger (associate director for Strategic Planning, USAF HQ) toteaa, että seuraavaa sotateknologista vallankumousta johtaa ja ohjaa suunnatun energian aseiden kehitys. Operatiivisen suorituskyvyn katsotaan kehittyvän suunnatun energian aseiden lisäksi täsmäammuksista (PGM), miniatyyriammuksista, häiveteknologiasta, jatkuvasta tiedustelusta ja valvonnasta (persistent ISR) sekä laajakaistaisesta tiedonsiirtoalustasta. Nick Cook: *Cause and Effect*, Jane's Defense Weekly 18.6.2003.

[65] Terroristien ja sissien käyttämien leluista, autotalliovien sekä televisioiden/radioiden kaukosäätimistä yms. kaupallisesta elektroniikasta viritettyjen pommien etälaukaisimien torjuminen pienikokoisilla häirintäjärjestelmillä sai runsaasti huomiota vuoden 2003 Irakin sodan jälkimainingeissa. Häirintäjärjestelmiä myydään runsaasti myös siviilikäyttöön. Sinänsä menetelmä ei ole uusi: Suomalaiset estivät venäläisten radiolaukaistavien miinojen toimintaa jatkosodassa elektronisella häirinnällä. William Matthews: *Boom Time for Bomb Jammers*, Defense News 22.3.2004. s. 30.

[66] Ted McKenna: *Hearing Impaired*. The Journal of Electronic Defense, elokuu 2004, ss. 36-41.

[67] Esimerkkejä elektroniseen sodankäyntiin liittyvistä laskuista, etenkin tutka- ja häirintäjärjestelmiin liittyvistä, on hankala esittää julkisessa oppimateriaalissa, koska laskuissa tarvittavia järjestelmien ominaisuuksia ei yleensä ole julkisesti saatavilla. Harvinainen ja laaja taulukko todellisten järjestelmien ominaisuuksista on esitetty kirjassa David Lynch Jr: *Introduction to RF Stealth*, ISBN 0-86341-349-8, SciTech Publishing Inc. 2004 (ss. 265-273). Koska lähde on julkinen, sen tarkkuuteen on näinkin sensitiivisen asian vuoksi suhtauduttava erittäin kriittisesti. ELSO:n perusrelaatioiden ymmärtämiseen tarkkuus riittänee.

[68] Michael Sirak: *US vulnerable to EMP attack*. Jane's Defence Weekly 28.7.2004.

[69] Jyri Kosola: *Suurtehomikroaaltoase ja perusteet siltä suojautumiselle*. Maanpuolustuskorkeakoulun Tekniikan Laitoksen julkaisu 2000: Tutkimuksia, julkaisusarja 1, No. 6. Julkaisu kuvaa radiotaajuisten aseiden toimintaperiaatteet ja niiden muodostaman uhkan sekä esittää mekanismeja, joilla suojautumista voidaan kehittää.

[70] US Army Field Manual FM 100-60 -sarja. Useat näistä ja muuta tukevaa dokumentaatiota löytyy Internetistä osoitteesta http://www.train.army.mil.